НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз функціональних компонентів безпеки інформаційних систем та технологій»

Виконав:
студент III курсу, групи ТС-п71
Савченко Дмитро Олегович _____

Керівник:
Професор кафедри ТС, д.т.н., професор
Горицький Віктор Михайлович _____

Рецензент:

_____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«__»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Савченко Дмитро Олегович

1. Тема роботи «Аналіз функціональних компонентів безпеки інформаційних систем та технологій», керівник роботи Горицький Віктор Михайлович, д.т.н., проф. кафедри, затверджені наказом по університету від 30 березня 2020 р. № 924-с

2. Термін подання студентом роботи 12 червня 2020 р.

3. Вихідні дані до роботи

1) Загальна модель оцінки безпеки інформаційних хнологій;

2) Міжнародний стандарт ISO/IEC 15408 та його застосування;

2) ПЗ, ЗБ, ОО, ОРД, СкПД;

3) Структура функціональних класів-сімейств-компонентів та структура класів-сімейств-компонентів довіри до безпеки;

4) методи оцінки, взаємозв'язок вимог і рівня довіри.

4. Зміст роботи

1) Оціночні стандарти в області інформаційної безпеки

2) Функціональні компоненти безпеки технологій.

3) Аналіз функціональних класів

4) Сертифікація

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Дата видачі завдання 12.12.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Прим.
1	Підбір науково-технічної літератури	12.12.19-15.12.19	
2	Обгрунтування актуальності теми роботи	15.12.19-21.02.19	
3	Написання першого розділу роботи, а саме описав деякі оціночні стандарти.	21.02.20-11.05.20	
4	Написання другого розділу роботи, а саме описав структуру функціонального компоненту. А також опрацював четвертий розділ диплому «сертифікація»	11.05.20-01.06.20	
5	Написання третього розділу роботи, а саме описав функціональні компоненти безпеки.	01.06.20-28.08.20	
6	Написання висновків по роботі	28.08.20-25.09.20	
7	Підготовка демонстраційних матеріалів	25.09.20-23.10.20	
8	Підготовка доповіді	23.10.20-27.11.20	

Студент Дмитро САВЧЕНКО

Керівник роботи Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Темою дипломної роботи є аналіз функціональних компонентів безпеки інформаційних систем та технологій

Робота містить 78 сторінок, зокрема 20 ілюстрації та 8 джерел інформації.

Тема дипломної роботи є актуальною, так як інформаційна безпека є важливим фактором, з розвитком інформаційних технологій все частіше намагаються отримати несанкціонований доступу до даних, в свою чергу яке може призвести до великих втрат.

Мета дипломної роботи в аналізі уже доступних функціональних компонентів, аналіз міжнародних стандартів в сфері інформаційної безпеки.

Об’єктом дослідження є інформаційна безпека.

Предметом дослідження є функціональні компоненти інформаційної безпеки.

При виконанні роботи проводився аналіз доступних рекомендацій по критеріям оцінки безпеки.

STANDARD, FUNCTIONAL COMPONENTS, CLASS, CERTIFICATION, ISO 15408, SAFETY COMPONENTS

ABSTRACT

The topic of the thesis is the analysis of functional components of security of information systems and technologies

The work contains 78 pages, in particular 20 illustrations and 8 sources of information.

The topic of the thesis is relevant, as information security is an important factor, with the development of information technology increasingly trying to gain unauthorized access to data, which in turn can lead to large losses.

The purpose of the thesis in the analysis of already available functional components, analysis of international standards in the field of information security.

The object of research is information security.

The subject of research is the functional components of information security.

When performing the work, an analysis of available recommendations on safety assessment criteria was performed.

STANDARD, FUNCTIONAL COMPONENTS, CLASS, CERTIFICATION, ISO 15408, SAFETY COMPONENTS

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ФБ - функція безпеки

ЗБ - завдання з безпеки

ПФБ - політика функцій безпеки

ТЗІ - технічний захист інформації

ЗТЗІ - засіб технічного захисту інформації

ІТ - інформаційна технологія

ОВЗ - особа, що виконує зіставлення

ФБО - функції безпеки об’єкта оцінювання

ФБП - функціональна послуга безпеки

ОДФ - область дії функцій безпеки об’єкта оцінювання

ІТС - інформаційно-телекомунікаційна система

КЗЗ - комплекс засобів захисту

КСЗІ - комплексна система захисту інформації

НД - нормативний документ

НСД - несанкціонований доступ

ОЕ - об'єкт експертизи

ОО - об’єкт оцінювання

ПБО - політика безпеки об’єкта оцінювання

ПЗ - профіль захисту

ВСТУП

В даний час людина живе в інформаційному суспільстві і активно бере участь в інформаційних процесах. І немає нічого дивного в тому що на безпеку інформації може хтось зазіхати. Таким чином, перед суспільством постає завдання забезпечення інформаційної безпеки.

З метою формування єдиного і формалізованого підходу до захисту інформації були розроблені стандарти оцінки безпеки або критерії оцінки захищеності, які включають якісні і кількісні показники захищеності.

Сьогодні ми розберемо один з найбільш значущих в цьому плані документів – міжнародному стандарту ISO / IEC 15408 “Критерії оцінки безпеки інформаційних технологій”

У створенні цього стандарту брали участь різні організації з Канади, Англії, Франції, США, Німеччини, Голландії. У стандарті докладно розглянуті загальні підходи, методи та функції забезпечення захисту інформації.

Документами, які лягли в основу:

-Помаранчева книга (TCSEC) 1985р.;

-Європейські критерії (ITSEC) 1991р.;

-Канадські критерії 1993р.;

-Федеральні критерії США 1993р.

Функції системи інформаційної безпеки забезпечують виконання вимог цілісності, достовірності, конфіденційності та доступності інформації.

У стандарті виділені 11 класів функцій: аудит, ідентифікація та автентифікація, криптографічний захист, передача даних, захист даних користувача, захист функцій безпеки системи, управління безпекою, використання ресурсів, конфіденційність, надійність засобів, доступ до системи.

У стандарті міститься ряд моделей (профілів), що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі

поширених засобів захисту власноруч, а скористуватися вже готовими наборами цілей, описів, вимог і функцій до цих засобів.

У ньому проведена класифікація широкого набору функціональних вимог довіри і безпеки, визначені структури їх групування і принципи цільового використання.

Стандарт ISO/IEC 15408 описує інфраструктуру в якій розробники можуть заявити про властивості безпеки продуктів, користувачі комп’ютерної системи можуть описати вимогу, а експерти визначити, чи відповідає продукт заявам.

1 ОЦІНОЧНІ СТАНДАРТИ В ОБЛАСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стандарти в області інформаційної безпеки можна розділити на два класи:

- Оціночні стандарти, спрямованих на класифікацію інформаційних систем і засобів захисту за вимогами безпеки;

- Стандарти, які регламентують різні аспекти реалізації засобів захисту

1.1 «Помаранчева книга» "Критерії оцінки довірених комп'ютерних систем"

Історично першим оцінним стандартом, який отримав широке поширення і зробив величезний вплив на базу стандартизації ІБ в багатьох країнах, став стандарт Міністерства оборони США "Критерії оцінки довірених комп'ютерних систем".

Дана праця, званий найчастіше за кольором обкладинки "; Помаранчевої книгою" ;, був вперше опублікований в серпні 1983 року.

Звернемо увагу, що в розглянутих Критеріях і безпеку, і довіру оцінюються виключно з точки зору управління доступом до даних, що є одним із засобів забезпечення конфіденційності і цілісності (статичної). Питання доступності "; Помаранчева книга"; торкається.

Як видно з назви мова йде не про безпечні, а про довірених системах, тобто системах, яким можна надати певну ступінь довіри.

Довірена система - система, яка використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу.

Також важливою є концепція Довіреною обчислювальної бази є центральною при оцінці ступеня довіри безпеки. Довірена обчислювальна база - це сукупність захисних механізмів АС (включаючи апаратне і програмне забезпечення), що відповідають за проведення в життя політики

безпеки. Якість обчислювальної бази визначається виключно її реалізацією і коректністю вихідних даних, які вводить системний адміністратор.

Роль монітора безпеки в «Помаранчевої книзі» Основне призначення довіреної обчислювальної бази - виконувати функції монітора звернень. Функції монітора звернень - контролювати допустимість виконання суб'єктами доступу певних операцій над об'єктами доступу. Монітор перевіряє кожне звернення користувача до програм або даними на предмет узгодженості з набором дій, допустимих для користувача.

Обов'язкові властивості Монітору звернень:

- Ізольованість. Необхідно попередити можливість відстеження роботи монітора.

- Повнота. Монітор повинен викликатися при кожному зверненні, не повинно бути способів обійти його.

- Верифіковані. Монітор повинен бути компактним, щоб його можна було проаналізувати і протестувати, будучи впевненим у повноті тестування.

Методи забезпечення інформаційної безпеки:

- Дискреційне управління доступом;

- Безпеку повторного використання об'єктів;

- Використання міток безпеки;

- Примусове управління доступом.

Дискреційне управління доступом - здатність власника (або іншої людини, який отримав відповідні повноваження) визначати правила доступу до об'єкта доступу.

Безпека повторного використання об'єктів - Можливість виключити витяг конфіденційної інформації з місць її проміжного зберігання (оперативна пам'ять для буферів з образами екрана, і т.п.)

Використання міток безпеки - кожен об'єкта доступу - повинен мати мітку доступу описує ступінь конфіденційності міститься в ньому інформації.

Примусове (або мандатний) управління доступом - зіставленні міток безпеки суб'єкта й об'єкта доступу, для прийняття рішення надано доступ.

Суб'єкт може читати інформацію з об'єкта, якщо рівень секретності суб'єкта не нижче, ніж у об'єкту, а всі категорії, перераховані в мітці безпеки об'єкта, присутні в мітці суб'єкта. У такому випадку говорять, що мітка суб'єкта домінує над міткою об'єкта. Сенс сформульованого правила зрозумілий - читати можна тільки те, що належить.

Класи безпеки згідно " Помаранчевої книзі"

"Критерії"; Міністерства оборони США відкрили шлях до ранжирування інформаційних систем за ступенем довіри безпеки.

В "Помаранчевої книзі" визначається чотири рівні довіри - D, C, B і A. Рівень D призначений для систем, визнаних незадовільними. У міру переходу від рівня C до A до систем пред'являються все більш жорсткі вимоги. Рівні C і B поділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Всього є шість класів безпеки - C1, C2, B1, B2, B3, A1. Щоб в результаті процедури сертифікації систему можна було віднести до певного класу, її політика безпеки і рівень гарантованості повинні задовольняти заданим вимогам.

1.2 ISO 15408 "Критерії оцінки безпеки інформаційних технологій", 1 грудня 1999 року

ISO / IEC 15408 є метастандартом, визначальним інструменти оцінки безпеки АС і порядок їх використання. На відміну від "; Помаранчевої книги" ISO/IEC 15408 не містять зумовлених " класів безпеки" Такі класи можна будувати, виходячи з вимог безпеки, що існують для конкретної організації і / або конкретної автоматизованої системи. Дуже важливо, що безпека в ISO / IEC 15408 розглядається не статично, а в прив'язці до життєвого циклу об'єкта оцінки. Виділяються наступні етапи:

- визначення призначення, умов застосування, цілей і вимог безпеки;
- проектування і розробка;
- випробування, оцінка та сертифікація;
- впровадження і експлуатація.

Функціональні вимоги згруповані на основі виконуваної ними ролі або обслуговується цілі безпеки. Всього в "; Загальних умовах"; представлено 11 функціональних класів, 66 родин, 135 компонентів. Це, звичайно, значно більше, ніж число аналогічних сутностей в "Помаранчевої книзі".

1.3 Стандарт інформаційна безпека розподілених систем «Рекомендації X.800»

Ця специфікація з'явилася трохи пізніше "Помаранчевої книги", але дуже повно і глибоко трактує питання інформаційної безпеки розподілених систем.

Виділяють наступні сервіси безпеки і виконувані ними ролі (за версією X.800):

- Автентифікація. Даний сервіс забезпечує перевірку автентичності партнерів по спілкуванню і перевірку автентичності джерела даних. Аутентифікація партнерів по спілкуванню використовується при встановленні з'єднання і, можливо, періодично під час сеансу. Вона служить для запобігання таких загроз, як маскарад і повтор попереднього сеансу зв'язку. Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність серверу) і двосторонньої (взаємної).

- Управління доступом. Забезпечує захист від несанкціонованого використання ресурсів, доступних через мережу.

- Конфіденційність даних. Забезпечує захист від несанкціонованого отримання інформації. Окремо згадаємо конфіденційність трафіку (це захист інформації, яку можна отримати, аналізуючи мережеві потоки даних).

- Цілісність даних поділяється на підвиди залежно від того, який тип спілкування використовують партнери - з встановленням з'єднання або без нього, захищаються чи всі дані або тільки окремі поля, чи забезпечується відновлення в разі порушення цілісності.

- Неспростовності (неможливість відмовитися від вчинених дій) забезпечує два види послуг: неспростовності з підтвердженням справжності джерела даних і неспростовності з підтвердженням доставки. Побічним продуктом неспростовності є автентифікація джерела даних.

1.4 Висновки до розділу 1

Можемо зробити висновок що використання стандартів допомагає вирішити наступні завдання:

- Створення ефективної системи управління інформаційною безпекою.

- Визначити цілі забезпечення інформаційної безпеки комп'ютерних систем.

- Надається можливість використання методик управління безпекою з обґрунтованою системою метрик і заходів забезпечення розробників інформаційних систем.

- Надається розрахунок сукупності кількісних та якісних показників для оцінки відповідності інформаційної безпеки заявленим цілям.

- Створенню умов застосування наявного інструментарію, програмних засобів, забезпечення інформаційної безпеки і оцінки її поточного стану.

2 ФУНКЦІОНАЛЬНІ КОМПОНЕНТИ БЕЗПЕКИ

2.1 Структура класу

Структура функціонального класу наведена на рис. 3. Кожен функціональний клас містить ім'я класу, представлення класу і одне або кілька функціональних сімейств.

Рисунок 2.1 - Структура функціонального класу

2.1.1 Ім'я класу

Ім'я класу містить інформацію, необхідну для ідентифікації функціонального класу і віднесення його до певної категорії. Кожен функціональний клас має унікальне ім'я. Інформація про категорії надана коротким ім'ям, що складається з трьох букв латинського алфавіту. Коротке ім'я класу використовують при завданні коротких імен сімейств цього класу.

2.1.2 Подання класу

Подання класу узагальнює участь сімейств класу в досягненні цілей безпеки. Визначення функціональних класів не відображає ніякої формальну таксономію в специфікації вимог.

Подання класу містить рисунок, що показує всі сімейства цього класу і ієрархію компонентів в кожному сімействі, як зазначено в підрозділі

2.2 Структура сімейства

Структура функціонального сімейства приведена на рис. 2.2

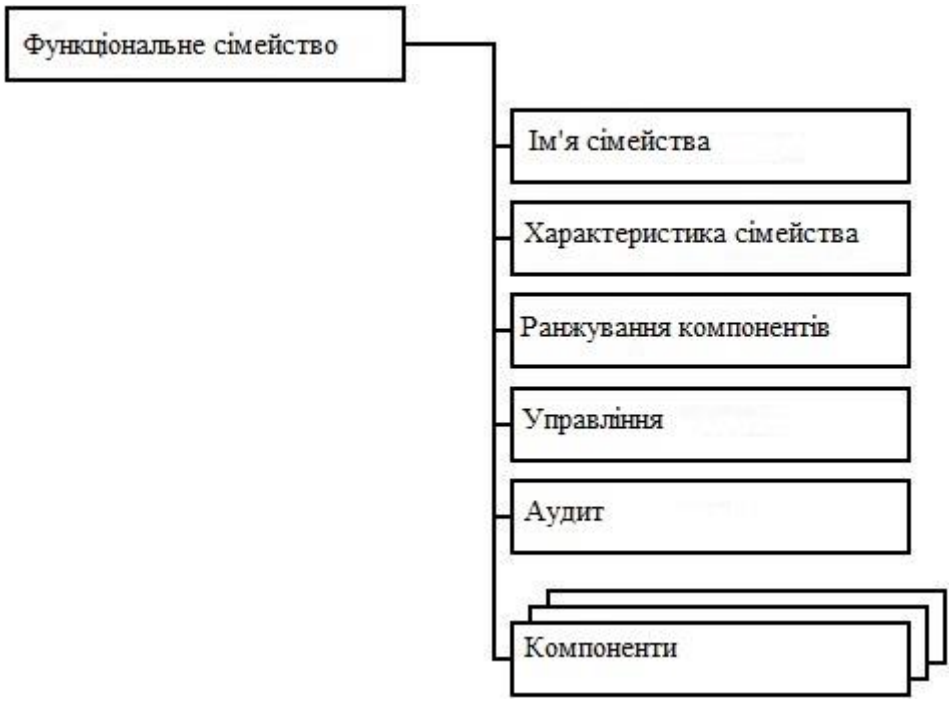


Рисунок 2.2 - Структура функціонального сімейства

2.2.1 Ім'я сімейства

Ім'я сімейства містить описову інформацію, необхідну, щоб ідентифікувати і категоризувати функціональне сімейство. Кожне

функціональне сімейство має унікальне ім'я. Інформація про категорії складається з короткого імені, що включає в себе сім символів. Перші три символи ідентичні короткому імені класу, далі йдуть символ підкреслення і коротке ім'я сімейства у вигляді XXX_YYY. Унікальна коротка форма імені сімейства надає основне ім'я посилання для компонентів

2.2.2 Характеристика сімейства

Характеристика сімейства - це опис функціонального сімейства, в якому викладаються його цілі безпеки і загальний опис функціональних вимог. Більш детально вони описані нижче:

a) цілі безпеки сімейства характеризують задачу безпеки, яка може бути вирішена за допомогою компонентів цього сімейства;

b) опис функціональних вимог узагальнює всі вимоги, які включені в компонент (ті). Опис орієнтований на розробників ПЗ, ЗБ і функціональних пакетів, які хотіли б визначити, чи відповідає сімейство їх конкретним вимогам.

2.2.3 Ранжування компонентів

Функціональні сімейства містять один або кілька компонентів, кожен з яких може бути обраний для включення в ПЗ, ЗБ і функціональні пакети. Мета ранжирування компонентів - надати користувачам інформацію для вибору підходящого функціонального компонента, якщо сімейство ідентифіковано користувачем як необхідна або корисна частина вимог безпеки.

Далі перераховуються наявні компоненти і наводиться їх обгрунтування. Деталізація компонентів здійснюється в описі кожного компонента.

Зв'язки між компонентами в межах функціонального сімейства можуть бути ієрархічними і не ієрархічні. Компонент є ієрархічним (тобто розташований вище по ієрархії) по відношенню до іншого компоненту, якщо пропонує більшу безпеку.

Описання сімейств містять графічне представлення ієрархії компонентів.

2.2.4 Управління

Пункти "Управління" містять інформацію для розробників ПЗ / ЗБ, що враховується при визначенні дій з управління для даного компонента. Дані пункти посилаються на компоненти класу "Управління безпекою" (FMT) і надають керівництво щодо потенційних видів діяльності з управління, які через виконання операцій можуть бути відображені в даних компонентах.

Розробник ПЗ / ЗБ може вибрати будь-які із зазначених компонентів управління або включити нові, не зазначені в цьому стандарті. В останньому випадку має бути поданий необхідну інформацію.

2.2.5 Аудит

Вимоги аудиту містять події, потенційно піддаються аудиту, для їх відбору розробниками ПЗ / ЗБ за умови включення в ПЗ / ЗБ вимог з класу FAU "Аудит безпеки". Ці вимоги включають в себе події, які стосуються безпеки, стосовно до різних рівнів деталізації, підтримуваним компонентами сімейства FAU_GEN "Генерація даних аудиту безпеки". Наприклад, запис аудиту будь-якого механізму безпеки може включати в себе на різних рівнях деталізації дії, які розкриваються в наступних термінах:

- Мінімальний - успішне використання механізму безпеки.

- Базовий - будь-яке використання механізму безпеки, а також інформація про поточні значення атрибутів безпеки.

- Деталізований - будь-які зміни конфігурації механізму безпеки, включаючи параметри конфігурації до і після зміни.

Слід врахувати, що категоризування подій, потенційно піддаються аудиту, завжди ієрархічно. Наприклад, якщо обрана базова генерація даних аудиту, то всі події, ідентифіковані як потенційно піддаються аудиту і тому входять як в "мінімальну", так і в "базову" запис, слід включити в ПЗ / ЗБ за допомогою відповідної операції призначення, за винятком випадку , коли подія більш високого рівня має більш високий рівень деталізації, ніж подія нижчого рівня, і може просто замінити його. Коли бажана деталізована генерація даних аудиту, все ідентифіковані події, потенційно піддаються аудиту (для мінімального, базового і детального рівнів), слід включити в ПЗ/ЗБ.

Правила управління аудитом більш докладно пояснені в класі FAU "Аудит безпеки".

2.2.6 Структура компонента

Структура функціонального компонента показана на рис. 2.3

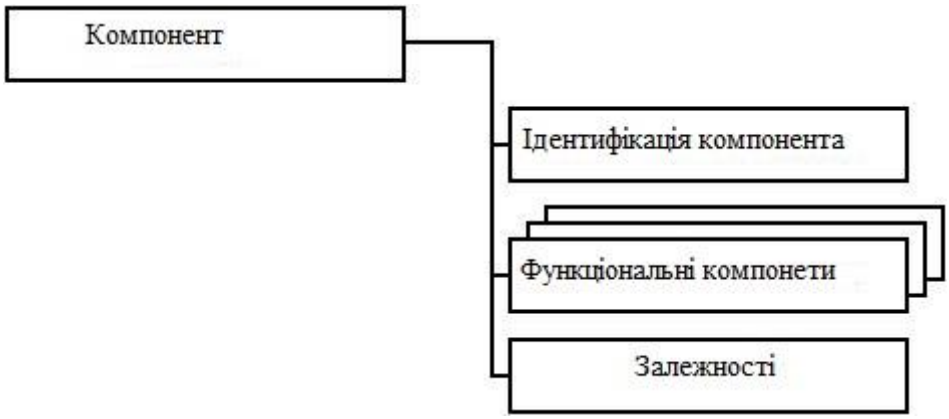


Рисунок 2.3 - Структура функціонального компонента

2.2.7 Ідентифікація компонента

Ідентифікація компонента містить у собі описову інформацію,

необхідну для ідентифікації, категоризування, записи і реалізації перехресних посилань компонента. Для кожного функціонального компонента представляється наступне:

- унікальне ім'я, що відбиває призначення компонента;

- коротке ім'я, яке використовується як основне ім'я посилання для категоризування, записи і реалізації перехресних посилань компонента і унікально відображає клас і сімейство, яким компонент належить, а також номер компонента в сімействі;

- список ієрархічних зв'язків, що містить імена інших компонентів, для яких цей компонент ієрархічний і замість яких може використовуватися при задоволенні залежності від перерахованих компонентів.

2.2.8 Функціональні елементи

Кожен компонент включає в себе набір елементів. Кожен елемент визначається окремо і є самодостатнім.

Функціональний елемент - це функціональне вимога безпеки, подальший поділ якого не змінює значимо результат оцінки. Є найменшим функціональним вимогам безпеки, які можуть бути ідентифіковані та визнаним в ISO / IEC 15408.

При формуванні ПЗ, ЗБ і / або пакетів не дозволяється вибирати тільки частина елементів компонента. Для включення в ПЗ, ЗБ або пакет необхідно вибирати всю сукупність елементів компонента.

Вводиться унікальна коротка форма імені функціонального елемента. Наприклад, ім'я FDP_IFF.4.2 читається так:

F - функціональне вимога,

DP - клас "Захист даних користувача",

_IFF - сімейство "Функції управління інформаційними потоками",

4 (після крапки) - четвертий компонент "Часткове усунення невирішених інформаційних потоків",

2 (після крапки) - другий елемент компонента.

2.2.9 Залежності

Залежно серед функціональних компонентів виникають, коли компоненти не самодостатній і потребує або функціональні можливості іншого компонента, або у взаємодії з ним для підтримки власного виконання.

Кожен функціональний компонент містить повний список залежностей від інших функціональних компонентів і компонентів довіри. Для деяких компонентів вказано, що залежно відсутні. Компоненти зі списку можуть, в свою чергу, мати залежності від інших компонентів. Список, наведений в компоненті, показує прямі залежності, тобто містить посилання тільки на функціональні компоненти, свідомо необхідні для забезпечення виконання даного компонента. Непрямі залежності, які визначаються власними залежностями компонентів зі списку, показані в додатку А. У деяких випадках залежність вибирають з декількох запропонованих функціональних компонентів, причому кожен з них достатній для задоволення залежності (див., Наприклад, FDP_UIT.1 "Цілісність переданих даних").

Список залежностей ідентифікує мінімум функціональних компонентів або компонентів довіри, необхідних для задоволення вимог безпеки, асоційованих з даними компонентом. Компоненти, які ієрархічно по відношенню до компоненту зі списку, також можуть бути використані для задоволення залежності.

Залежності між компонентами, зазначені в цьому стандарті, обов'язкові. Їх необхідно задовольнити в ПЗ / ЗБ. У деяких, особливих,

випадках ці залежності задовольнити неможливо. Розробник ПЗ/ЗБ, обов'язково обгрунтувавши, чому дана залежність не може бути застосована, може не включати відповідний компонент в пакет, ПЗ або ЗБ.

2.2.10 Каталог компонентів

Розташування компонентів в цьому стандарті не відображає будь-яку формальну таксономію.

Цей стандарт містить класи, що складаються з родин і компонентів, які приблизно згруповані на основі загальної функції і призначення. Класи і сімейства представлені в алфавітному (латинською) порядку. На початку кожного класу є рисунок, що показує таксономію цього класу, перераховуючи сімейства в цьому класі і компоненти в кожному сімействі. Рисунок також ілюструє ієрархію компонентів всередині кожного сімейства.

В описі кожного функціонального компонента наведені його залежності від інших компонентів.

Приклад подання таксономії класу і ієрархії компонентів в його родинах наведено на рис. 2.4.

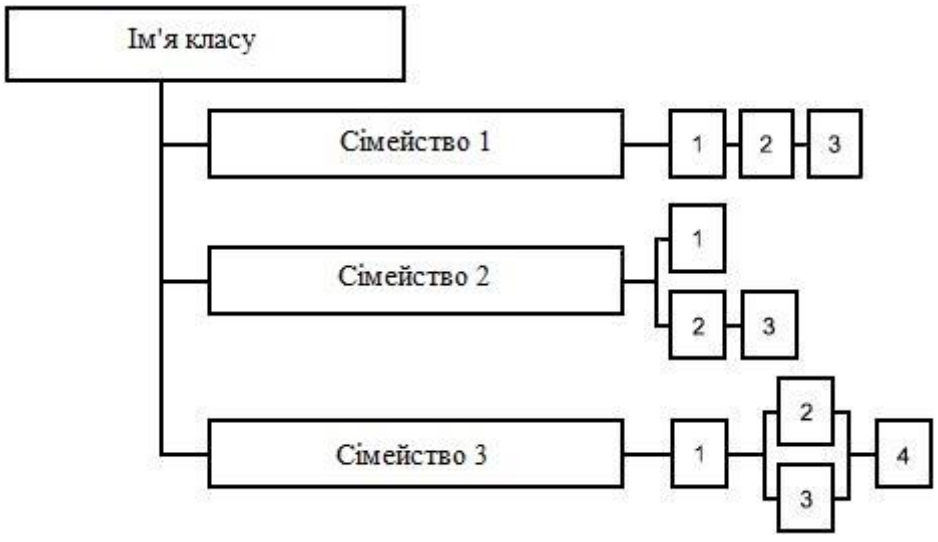


Рисунок 2.4 - Приклад декомпозиції класу

На рис. 2.10 сімейство 1 містить три ієрархічних компонента, де компоненти 2 і 3 можуть бути застосовані для виконання залежностей замість компонента 1. Компонент 3 ієрархічний до компоненту 2 і може застосовуватися для виконання залежностей замість компонента 2.

У сімействі 2 є три компоненти, не всі з яких ієрархічно пов'язані. Компоненти 1 і 2 цієї статті не ієрархічні до інших компонентів. Компонент 3 ієрархічний до компоненту 2 і може застосовуватися для задоволення залежностей замість компонента 2, але не замість компонента 1.

У сімействі 3 компоненти 2, 3 і 4 ієрархічні до компоненту 1. Компоненти 2 і 3 ієрархічні до компоненту 1, але не можна порівняти за ієрархією між собою. Компонент 4 ієрархічний до компонентів 2 і 3.

Подібні рисунки доповнюють текст опису сімейств і роблять простіше ідентифікацію відносин їх компонентів. Вони не замінюють пункт "Ієрархічний для" в описі кожного компонента, який встановлює обов'язкові затвердження ієрархії для кожного компонента.

2.3 Висновок до розділу 2

В цьому розділі ми визначили зміст і форму структури функціональних компонентів захисту, «Клас» , «Сімейство» та «Компонент», розбили їх на складові частини та описали кожну з них.

3 АНАЛІЗ ФУНКЦІОНАЛЬНИХ КЛАСІВ

3.1 Клас FIA. Ідентифікація та автентифікація

Сімейства класу FIA містять вимоги до функцій встановлення і верифікації заявленого ідентифікатора користувача.

Ідентифікація та автентифікація потрібні для забезпечення асоціації користувачів з відповідними атрибутами безпеки (такими, як ідентифікатор, групи, ролі, рівні безпеки або цілісності).

Однозначна ідентифікація уповноважених користувачів і правильна асоціація атрибутів безпеки з користувачами та суб'єктами критичні для здійснення прийнятих політик безпеки. Сімейства цього класу пов'язані з визначенням і верифікацією ідентифікаторів користувачів, визначенням їх повноважень на взаємодію з ОО, а також з правильною асоціацією атрибутів безпеки з кожним уповноваженим користувачем. Ефективність вимог інших класів (таких, як "Захист даних користувача", "Аудит безпеки") багато в чому залежить від правильно проведених ідентифікації і автентифікації користувачів.

Декомпозиція класу FDP на складові його компоненти приведена на рис. 3.1.

Характеристика сімейства

Сімейство FIA_AFL містить вимоги до визначення числа неуспішних спроб автентифікації і до дій ФБО при перевищенні обмежень на неуспішні спроби автентифікації. Параметрами, що визначають можливе число спроб автентифікації, серед інших можуть бути кількість спроб і допустимий інтервал часу.

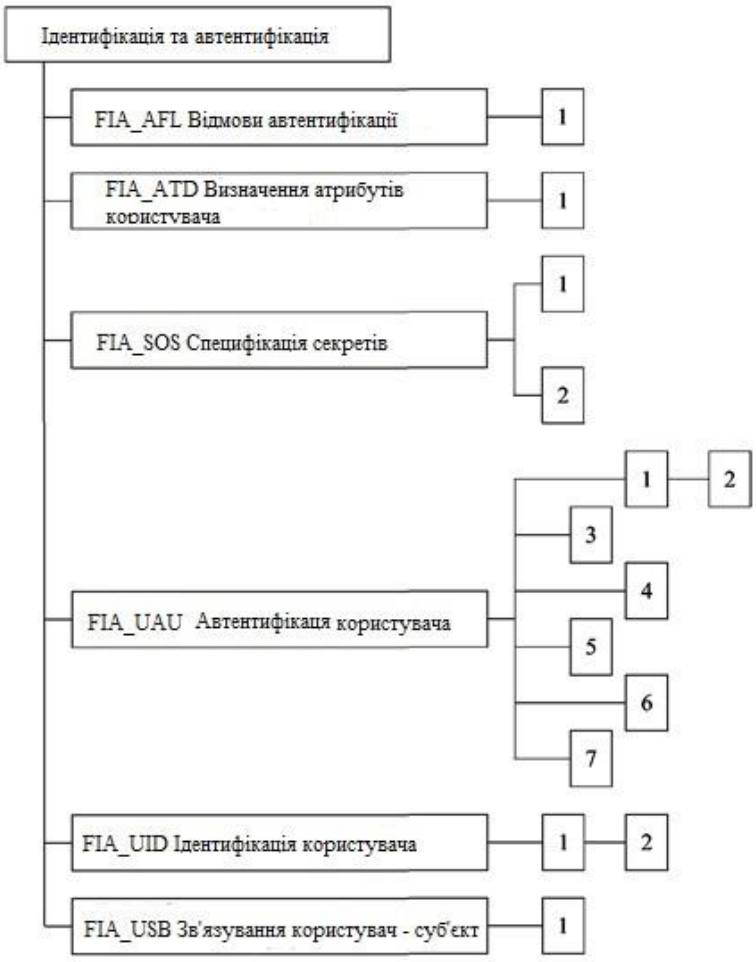


Рисунок 3.1 – Декомпозиція класу «Ідентифікація та автентифікація»

3.1.1 Відмови автентифікації (FIA_AFL)

Ранжування компонентів

FIA_AFL.1 "Обробка відмов автентифікації" містить вимогу, щоб ФБО були здатні перервати процес відкриття сеансу після певного числа неуспішних спроб автентифікації користувача. Також потрібно, щоб після переривання процесу відкриття сеансу ФБО були б здатні блокувати облікові дані користувача або місце входу (наприклад, робочу станцію), з якого виконувалися спроби, до настання визначеної адміністратором умови.

3.1.2 Визначення атрибутів користувача (FIA_ATD)

Характеристика сімейства

Всі уповноважені користувачі можуть, крім ідентифікатора користувача, мати інші атрибути безпеки, що застосовуються при здійсненні ПБО. Сімейство FIA_ATD визначає вимоги для асоціації атрибутів безпеки з користувачами відповідно до необхідності підтримки ПБО.

Ранжування компонентів

FIA_ATD.1 "Визначення атрибутів користувача" дозволяє підтримувати атрибути безпеки користувача для кожного користувача індивідуально.

3.1.3 Специфікація секретів (FIA_SOS)

Характеристика сімейства

Сімейство FIA_SOS визначає вимоги до механізмів, які реалізують певну метрику якості для наданих секретів і генерують секрети, що задовольняють певній метриці.

Ранжування компонентів

FIA_SOS.1 "Верифікація секретів" містить вимогу, щоб ФБО верифікували, чи відповідають секрети певної якості метрики.

FIA_SOS.2 "Генерація секретів ФБО" містить вимогу, щоб ФБО були здатні генерувати секрети, які відповідають певній якості метрики.

3.1.4 Автентифікація користувача (FIA_UAU)

Характеристика сімейства

Сімейство FIA_UAU визначає типи механізмів автентифікації користувача що надаються ФБО. Воно також визначає ті атрибути, на

яких необхідно базувати механізми автентифікації користувача.

Ранжування компонентів

FIA_UAU.1 "Вибір моменту автентифікації" дозволяє користувачеві виконати деякі дії до автентифікації користувача.

FIA_UAU.2 "Автентифікація до будь-яких дій користувача" містить вимогу, щоб користувачі пройшли автентифікацію перш, ніж ФБО дасть їм можливість робити які-небудь дії.

FIA_UAU.3 "Автентифікація, захищена від підробок" містить вимогу, щоб механізм автентифікації був здатний виявити автентифікаційні дані, які були фальсифіковані або скопійовані, і запобігти їхнього використання.

FIA_UAU.4 "Механізми одноразової автентифікації" містить вимогу наявності механізму автентифікації, який оперує автентифікаційними даними одноразового використання.

FIA_UAU.5 "Поєднання механізмів автентифікації" містить вимогу надання та застосування різних механізмів автентифікації користувачів в особливих випадках.

FIA_UAU.6 "Повторна автентифікація" містить вимогу можливості визначення подій, при яких необхідна повторна автентифікація користувача.

FIA_UAU.7 "Автентифікація з захищеної зворотним зв'язком" містить вимогу, щоб під час автентифікації користувачеві надавалася тільки обмежена інформація про неї.

3.1.5 Ідентифікація користувача (FIA_UID)

Характеристика сімейства

Сімейство FIA_UID визначає умови, при яких від користувачів вимагають ідентифікувати себе до виконання при посередництві ФБО будь-яких інших дій, що вимагають ідентифікації користувача.

Ранжування компонентів

FIA_UID.1 "Вибір моменту ідентифікації" дозволяє користувачеві виконати деякі дії перед своєю ідентифікацією з використанням ФБО.

FIA_UID.2 "Ідентифікація до будь-яких дій користувача" містить вимогу, щоб користувачі ідентифікували себе перш, ніж ФБО дозволять їм робити які-небудь дії.

3.1.6 Зв'язування користувач-суб'єкт (FIA_USB)

Характеристика сімейства

Для роботи з ОО автентифікований користувач зазвичай активізує будь-який суб'єкт. Атрибути безпеки цього користувача асоціюються (повністю або частково) з цим суб'єктом. Сімейство FIA_USB визначає вимоги щодо створення та супроводження асоціації атрибутів безпеки користувача з суб'єктом, що діє від імені користувача.

Ранжування компонентів

FIA_USB.1 "Зв'язування користувач-суб'єкт" містить вимогу супроводу асоціацію між атрибутами безпеки користувача та суб'єктом, що діє від імені користувача.

3.2 Клас FDP: Захист даних користувача

Клас FDP містить сімейства, що визначають вимоги до функцій безпеки ОО і політикам функцій безпеки ОО, пов'язаних із захистом даних користувача. Він розбитий на чотири групи родин, які перераховані нижче і застосовуються до даних користувача в межах ОО при їх імпорті, експорті та зберіганні, а також до атрибутів безпеки, прямо пов'язаних з даними користувача.

а) Політики функцій безпеки для захисту даних користувача:

- FDP_ACC "Політика управління доступом";

- FDP_IFC "Політика управління інформаційними потоками".

Компоненти цих сімейств дозволяють розробнику ПЗ / ЗБ іменувати політики функцій безпеки для захисту даних користувача і визначати область

дії цих політик, які необхідно співвіднести з цілями безпеки. Передбачається, що імена цих політик будуть використовуватися всюди в тих функціональних компонентах, які мають операцію, яка запитує призначення або вибір "ПФБ управління доступом" і / або "ПФБ управління інформаційними потоками". Правила, які визначають функціональні можливості іменованих ПФБ управління доступом і управління інформаційними потоками, будуть встановлені в родинах FDP_ACF і FDP_IFF відповідно.

б) Види захисту даних користувача:

- FDP_ACF "Функції управління доступом"
- FDP_IFF "Функції управління інформаційними потоками"
- FDP_ITT "Передача в межах ОО"
- FDP_RIP "Захист залишкової інформації"
- FDP_ROL "Відкат"
- FDP_SDI "Цілісність даних, що зберігаються"

в) Автономне зберігання, імпорт і експорт даних

- FDP_DAU "Автентифікація даних"
- FDP_ETC "Експорт даних за межі дії ФБО"
- FDP_ITC "Імпорт даних з-за меж дії ФБО"

Компоненти цих сімейств пов'язані з довіреної передачею даних в або з ОДФ.

г) Зв'язок між ФБО:

- FDP_UCT "Захист конфіденційності даних користувача при передачі між ФБО";
- FDP_UIT "Захист цілісності даних користувача при передачі між ФБО".

Компоненти цих родин визначають взаємодію між ФБО власне ОО і іншого довіреного продукту ІТ.

Декомпозиція класу FDP на складові його компоненти приведена на рис. 3.2 та 3.3.

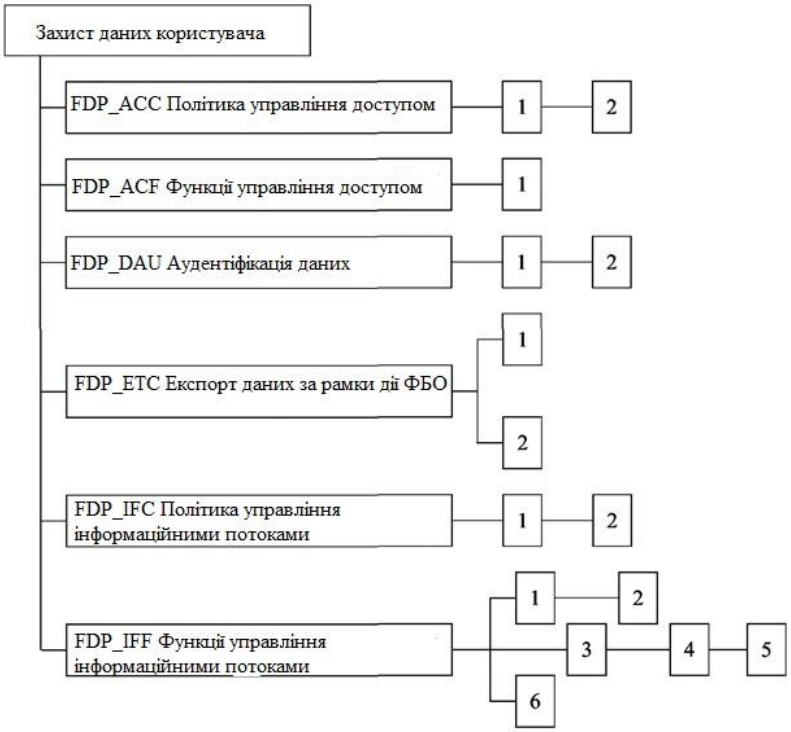


Рисунок 3.2 - Декомпозиція класу «Захист даних користувача»

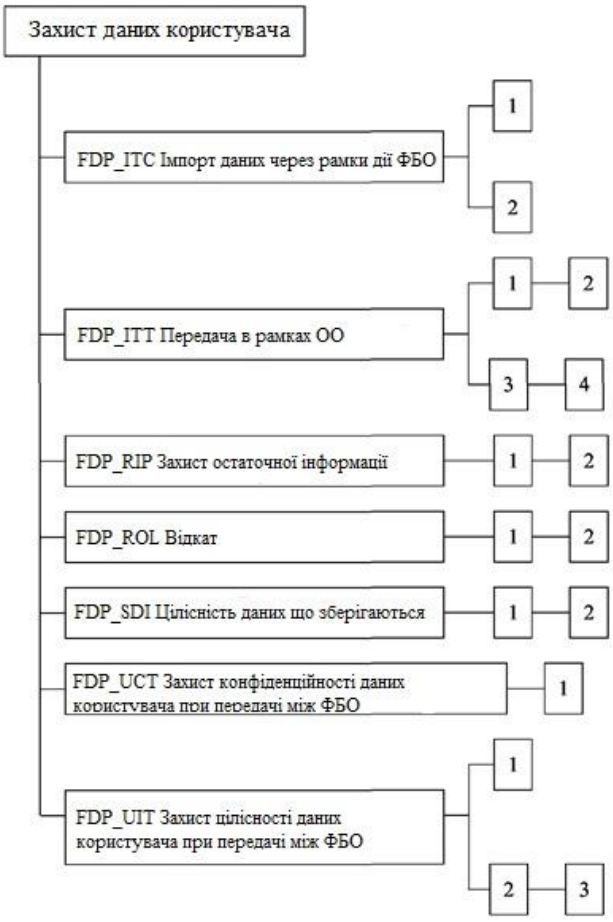


Рисунок 3.3 – Декомпозиція класу « Захист даних користувача»

3.2.1 Політика управління доступом (FDP_ACC)

FDP_ACC.1 Обмежене управління доступом

FDP_ACC.1.1 ФБО повинні здійснювати автентифікацію і контроль доступу до ОО для суб'єктів: Адміністратор кошти побудови ВЛВС; об'єктів: ОО, компоненти ОО; операцій: управління.

3.2.2 Функції управління доступом (FDP_ACF)

FDP_ACF.1 Управління доступом, що базується на атрибутах безпеки

FDP_ACF.1.1 ФБО повинні здійснювати аутентифікацію і контроль доступу до ОО до об'єктів, ґрунтуючись на ідентифікатор Адміністратора кошти побудови ВЛВС, паролі Адміністратора кошти побудови ВЛВС, ідентифікатор ВЛВС.

FDP_ACF.1.2 ФБО повинні реалізувати наступні правила визначення того, чи дозволено операція керованого суб'єкта на керований об'єкт: Локальне управління ОО або його компонентами можливо тільки за умови виконання наступних положень:

- на ОО повинна бути успішно проведена ідентифікація керованого суб'єкта (Адміністратора кошти побудови ВЛВС);
- на ОО повинна бути успішно проведена автентифікація керованого суб'єкта (Адміністратора кошти побудови ВЛВС).

FDP_ACF.1.2 ФБО повинні реалізувати наступні правила визначення того, чи дозволена операція керованого суб'єкта на керований об'єкт: Дистанційне керування ОО або його компонентами можливо тільки за умови виконання наступних положень:

- на ОО повинна бути успішно проведена ідентифікація керованого суб'єкта (Адміністратора кошти побудови ВЛВС);
- на ОО повинна бути успішно проведена автентифікація керованого суб'єкта (Адміністратора кошти побудови ВЛВС);

- вузол мережі керованого суб'єкта (Адміністратора кошти побудови ВЛВС) повинен належати певній ВЛВС (мати певне значення ідентифікатора ВЛВС).

FDP_ACF.1.3 ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, ґрунтуючись на наступних додаткових правилах: немає.

FDP_ACF.1.4 ФБО повинні явно відмовляти в доступі суб'єктів до об'єктів, ґрунтуючись на наступних правилах: немає.

3.2.3 Експорт даних за межі дії ФБО (FDP_ETC)

FDP_ETC.2 Експорт даних користувача з атрибутами безпеки

FDP_ETC.2.1 ФБО повинні здійснювати управління інформаційними потоками ВЛВС при експорті даних користувача, контрольованому ПФБ, за межі ОДФ.

FDP_ETC.2.2 ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача.

FDP_ETC.2.3 ФБО повинні забезпечити, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювалися з експортованими даними користувача.

FDP_ETC.2.4 ФБО повинні реалізувати наступні правила при експорті даних користувача з ОДФ: ОО повинен вставляти ідентифікатор ВЛВС в поле заголовка кадру даних, переданого іншого засобу побудови ВЛВС.

3.2.4 Політика управління інформаційними потоками (FDP_IFC)

FDP_IFC.1 Обмежене управління інформаційними потоками

FDP_IFC.1.1 ФБО повинні здійснювати управління інформаційними потоками ВЛВС для суб'єктів: зовнішніх об'єктів ІТ, що передають інформацію через ОО один одному; інформації: інформації, що проходить через ОО; операцій: передача інформації через ОО.

3.2.5 Функції управління інформаційними потоками (FDP_IFF)

FDP_IFF.1 Прості атрибути безпеки

FDP_IFF.1.1 ФБО повинні здійснювати управління інформаційними потоками ВЛВС, засноване на наступних типах атрибутів безпеки суб'єктів та інформації: суб'єктів: ідентифікатор ВЛВС, інші атрибути безпеки, специфіковані в ЗБ; інформації: ідентифікатор ВЛВС суб'єкта-відправника інформації, ідентифікатор ВЛВС суб'єкта-одержувача інформації, інші атрибути безпеки, специфіковані в ЗБ.

FDP_IFF.1.2 ФБО повинні дозволяти інформаційний потік між керованим суб'єктом і керованим об'єктом за допомогою керованої операції, якщо виконуються наступні правила: Передача інформації через ОО можлива тільки за умови виконання наступних положень:

- на ОО повинна бути успішно проведена ідентифікація суб'екта - відправника інформації (зовнішнього об'єкта ІТ);

- значення ідентифікатора ВЛВС суб'єкта-відправника інформації збігається зі значенням ідентифікатора ВЛВС суб'єкта-одержувача інформації.

Ґрунтуючись на наступних правилах: значення ідентифікатора ВЛВС суб'єкта-відправника інформації збігається зі значенням ідентифікатора ВЛВС суб'єкта-одержувача інформації.

FDP_IFF.1.6 ФБО повинні явно забороняти інформаційний потік, ґрунтуючись на наступних правилах: значення ідентифікатора ВЛВС суб'єкта-відправника інформації не збігається зі значенням ідентифікатора ВЛВС суб'єкта-одержувача інформації.

3.2.6 Імпорт даних з-за меж дій ФБО (FDP_ITC)

FDP_ITC.2 Імпорт даних користувача з атрибутами безпеки.

FDP_ITC.2.1 ФБО повинні здійснювати управління інформаційними потоками ВЛВС при імпорті даних користувача, контрольованому ПФБ, з-за меж ОДФ.

FDP_ITC.2.2 ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача.

FDP_ITC.2.3 ФБО повинні забезпечити, щоб використовуваний протокол зв'язку передбачав однозначну асоціацію між атрибутами безпеки і отриманими даними користувача.

FDP_ITC.2.4 ФБО повинні забезпечити, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача.

FDP_ITC.2.5 ФБО повинні реалізувати наступні правила при імпорті даних користувача, контрольованому ПФБ, з-за меж ОДФ: ОО повинен видаляти ідентифікатор ВЛВС з поля заголовка кадру даних, отриманих від іншого засобу побудови ВЛВС.

3.2.7 Захист залишкової інформації (FDP_RIP)

FDP_RIP.2 Повний захист залишкової інформації

FDP_RIP.2.1 ФБО повинні забезпечити недоступність будь-якого попереднього інформаційного змісту ресурсів при звільненні ресурсу

3.3 Клас FCS. Криптографічна підтримка

ФБО можуть використовувати криптографічні функціональні можливості для сприяння досягненню деяких, найбільш важливих цілей безпеки. До них відносяться (але ними не обмежуються) такі цілі:

ідентифікація і аутентифікація, неспростовності, довірений маршрут, довірений канал, поділ даних. Клас FCS застосовують, коли ОО має криптографічні функції, які можуть бути реалізовані апаратними, програмно-апаратними та / або програмними засобами.

Клас FCS складається з двох сімейств: FCS_CKM "Управління криптографічними ключами" і FCS_COP "Криптографічні операції". У сімействі FCS_CKM розглянуті аспекти управління криптографічними ключами, тоді як в сімействі FCS_COP розглянуто практичне застосування цих криптографічних ключів.

Декомпозиція класу FCS на складові його компоненти показана на рис. 3.4.

Рисунок 3.4 - Декомпозиція класу “Криптографічна підтримка”

3.3.1 Управління криптографічними ключами (FCS_CKM)

Характеристика сімейства

Криптографічними ключами необхідно керувати протягом усього їх життєвого циклу. Сімейство FCS_CKM призначене для підтримки життєвого циклу і тому визначає вимоги до наступних дій з криптографічними ключами: генерація, розподіл, доступ до них і їх знищення. Це сімейство слід

використовувати у випадках, коли є функціональні вимоги управління криптографічними ключами.

Ранжування компонентів

FCS_CKM.1 "Генерація криптографічних ключів" містить вимоги до їх створення відповідно до певного алгоритму і довжині ключа, які можуть ґрунтуватися на відповідному стандарті.

FCS_CKM.2 "Розподіл криптографічних ключів" містить вимогу їх розподілу певним методом, який може ґрунтуватися на відповідному стандарті.

FCS_CKM.3 "Доступ до криптографічних ключів" містить вимогу здійснення доступу до них згідно з визначеним методом, який може ґрунтуватися на відповідному стандарті.

FCS_CKM.4 "Знищення криптографічних ключів" містить вимогу їх знищення згідно з визначеним методом, який може ґрунтуватися на відповідному стандарті.

3.3.2 Криптографічні операції (FCS_COP)

Характеристика сімейства

Для коректного здійснення криптографічних операцій їх необхідно виконувати відповідно до певного алгоритму і з криптографічними ключами певної довжини. Дане сімейство слід застосовувати щоразу, коли необхідно виконувати криптографічні операції.

До типових криптографічним операцій належать: зашифрование і / або розшифрування даних, генерація і / або верифікація цифрових підписів, генерація криптографічних контрольних сум для забезпечення цілісності та / або верифікації контрольних сум, хешування (обчислення хеш-образу повідомлення), шифрування або розшифрування криптографічних ключів, узгодження криптографічних ключів.

Ранжування компонентів

FCS_COP.1 "Криптографічні операції" містить вимоги їх виконання за певними алгоритмами з застосуванням криптографічних ключів певної довжини. Алгоритми і довжина криптографічних ключів можуть ґрунтуватися на відповідному стандарті.

3.4 Клас FCO. зв'язок

Клас FCO містить два сімейства, пов'язані з упевненістю в ідентичності сторін, що беруть участь в обміні даними: ідентичністю відправника переданої інформації (доказ відправлення) та ідентичністю одержувача переданої інформації (доказ отримання). Ці родини забезпечують, що відправник не зможе заперечувати факт відправлення повідомлення, а одержувач не зможе заперечувати факт його отримання.

Декомпозиція класу на складові його компоненти показана на рис. 3.5

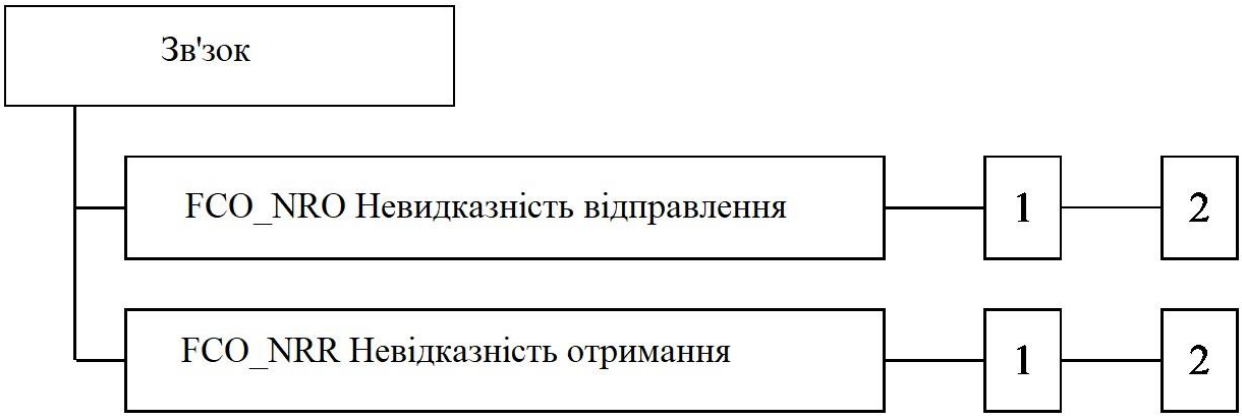


Рисунок 3.5 - Декомпозиція класу «зв’язок»

3.4.1 Неспростовність відправлення (FCO_NRO)

Характеристика сімейства

Сімейство FCO_NRO забезпечує неможливість заперечення відправником інформації факту її відправлення. Сімейство FCO_NRO

містить вимогу, щоб ФБО забезпечили метод надання суб'єкту-одержувачу свідоцтва відправлення інформації. Це свідоцтво може бути потім верифіковане цим суб'єктом або іншими суб'єктами.

Ранжування компонентів

FCO_NRO.1 "Виборчий доказ відправлення" містить вимогу, щоб ФБО надали суб'єктам можливість запросити свідоцтво відправлення інформації.

3.4.2 Неспростовність отримання (FCO_NRR)

Характеристика сімейства

Неспростовності отримання забезпечує неможливість заперечення одержувачем інформації факту її отримання. Сімейство FCO_NRR містить вимогу, щоб ФБО забезпечили метод надання суб'єкту-відправнику свідоцтва отримання інформації. Це свідоцтво може бути потім верифіковане цим суб'єктом або іншими суб'єктами.

Ранжування компонентів

FCO_NRR.1 "Вибірковий доказ отримання" містить вимогу, щоб ФБО надали суб'єктам можливість запросити свідоцтво отримання інформації.

FCO_NRR.2 "Примусовий доказ отримання" містить вимогу, щоб ФБО завжди генерували свідоцтво отримання прийнятої інформації.

3.5 Клас FAU. Аудит безпеки

Аудит безпеки включає в себе розпізнавання, запис, збереження та аналіз інформації, пов'язаної з діями, що стосуються безпеки (наприклад, з діями, контрольованими ПБО). Записи аудиту, одержувані в результаті, можуть бути проаналізовані, щоб визначити, які дії, пов'язані з безпекою, відбувалися, і хто з користувачів за них відповідає.

Декомпозиція класу на складові його компоненти показана на рис. 3.6

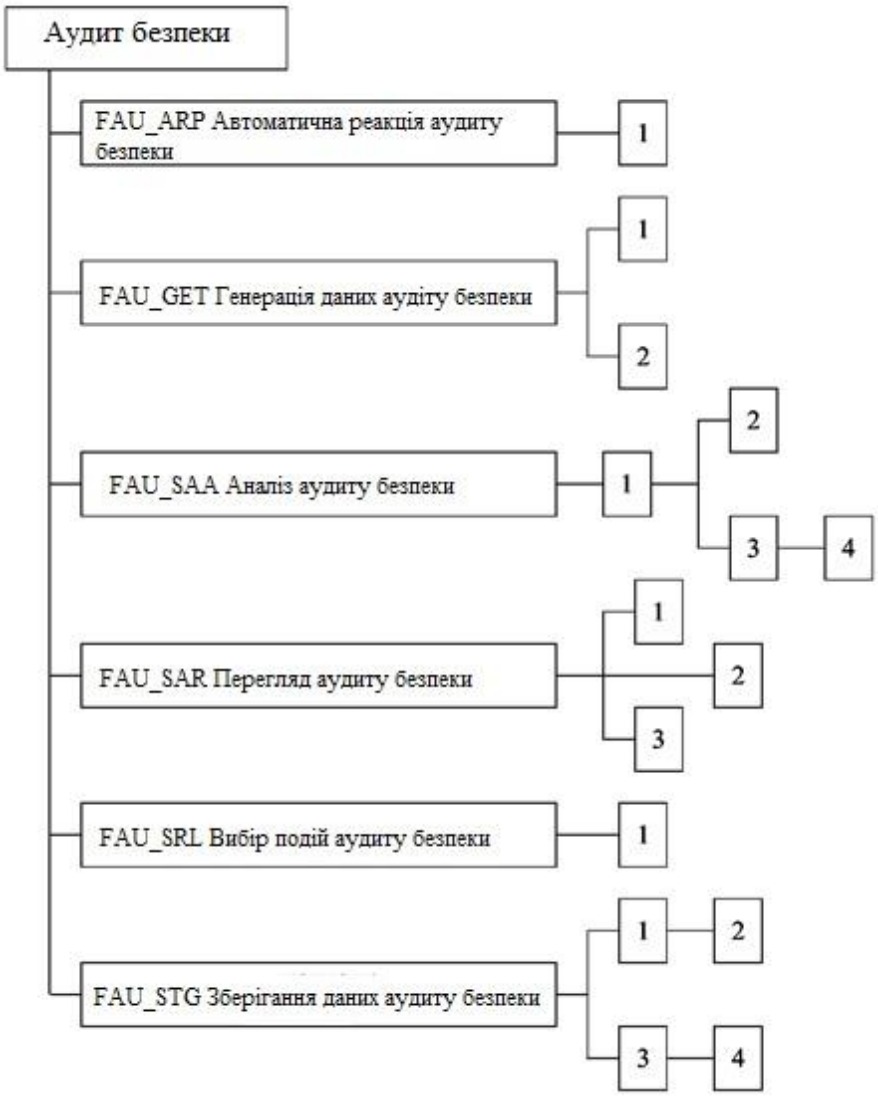


Рисунок 3.6 – Декомпозиція класу « Аудит безпеки»

3.5.1 Автоматична реакція аудиту безпеки (FAU_ARP)

Характеристика сімейства

Сімейство FAU_ARP визначає реакцію на виявлення подій, що вказують на можливе порушення безпеки.

Ранжування компонентів

У FAU_ARP.1 "Сигнали порушення безпеки" ФБО повинні вживати заходів у разі виявлення можливого порушення безпеки.

3.5.2 Генерація даних аудиту безпеки (FAU_GEN)

Характеристика сімейства

Сімейство FAU_GEN визначає вимоги щодо реєстрації виникнення подій, що відносяться до безпеки, які підконтрольні ФБО. Це сімейство ідентифікує рівень аудиту, перераховує типи подій, які потенційно повинні піддаватися аудиту з використанням ФБО, і визначає мінімальний обсяг пов'язаної з аудитом інформації, яку слід подавати в записах аудиту різного типу.

Ранжування компонентів

FAU_GEN.1 "Генерація даних аудиту" визначає рівень подій, які

потенційно піддаються аудиту, і склад даних, які повинні бути зареєстровані в кожному записі.

У FAU_GEN.2 "Асоціація ідентифікатора користувача" ФБО повинні асоціювати події, які потенційно піддаються аудиту, і особисті ідентифікатори користувачів.

3.5.3 Аналіз аудиту безпеки (FAU_SAA)

Характеристика сімейства

Сімейство FAU_SAA визначає вимоги для автоматизованих засобів, які аналізують показники функціонування системи і дані аудиту з метою пошуку можливих або реальних порушень безпеки. Цей аналіз може використовуватися для підтримки як виявлення проникнення, так і автоматичної реакції на очікуване порушення безпеки.

Дії, що вживаються при виявленні порушень, можуть бути при необхідності визначені з використанням сімейства FAU_ARP.

Ранжування компонентів

У FAU_SAA.1 "Аналіз потенційного порушення" потрібно базовий поріг виявлення на основі встановленого набору правил.

У FAU_SAA.2 "Виявлення аномалії, засноване на профілі" ФБО підтримують окремі профілі використання системи, де профіль являє собою шаблони передісторії використання, що виконувалися учасниками цільової групи профілю. Цільова група профілю може включати в себе одного або декількох учасників (наприклад, окремий користувач; користувачі, спільно використовують загальний ідентифікатор або загальні облікові дані, користувачі, яким призначено одна роль, і всі користувачі системи або мережного вузла), які взаємодіють з ФБО. Кожному учаснику цільової групи профілю призначається індивідуальний рейтинг підозрілої активності, який показує, наскільки поточні показники дій учасника відповідають встановленим шаблонами використання, представленим в профілі. Цей аналіз може виконуватися під час функціонування ОО або при аналізі даних аудиту в пакетному режимі.

У FAU_SAA.3 "Проста евристика атаки" ФБО повинні бути здатні виявити виникнення характерних подій, які свідчать про значну загрозу здійснення ПБО. Цей пошук характерних подій може відбуватися в режимі реального часу або при аналізі даних аудиту в пакетному режимі.

У FAU_SAA.4 "Складна евристика атаки" ФБО повинні бути здатні поставити і виявити багатокрокові сценарії проникнення. Тут ФБО здатні порівняти події в системі (можливо, що виконуються декількома учасниками) з послідовностями подій, відомими як повні сценарії проникнення. ФБО повинні бути здатні вказати на виявлення характерної події або послідовності подій, які свідчать про можливе порушення ПБО.

3.5.4 Перегляд аудиту безпеки (FAU_SAR)

Характеристика сімейства

Сімейство FAU_SAR визначає вимоги до засобів аудиту, до яких слід надати доступ уповноваженим користувачам для використання при перегляді даних аудиту.

Ранжування компонентів

FAU_SAR.1 "Перегляд аудиту" надає можливість читати інформацію із записів аудиту.

FAU_SAR.2 "Обмежений перегляд аудиту" містить вимогу відсутності доступу до інформації будь-кому, крім користувачів, зазначених в FAU_SAR.1.

FAU_SAR.3 "Вибірковий перегляд аудиту" містить вимогу, щоб кошти перегляду аудиту відбирали дані аудиту на основі критеріїв перегляду.

3.5.5 Вибір подій аудиту безпеки (FAU_SEL)

Характеристика сімейства

Сімейство FAU_SEL визначає вимоги для відбору подій, які будуть піддаватися аудиту під час функціонування ОО, а також вимоги для

включення або виключення подій з сукупності подій, що піддаються аудиту.

Ранжування компонентів

FAU_SEL.1 "Виборчий аудит" містить вимоги можливості включення або виключення події з сукупності подій, що піддаються аудиту, на основі атрибутів, що визначаються розробником ПЗ / ЗБ.

3.5.6 Зберігання даних аудиту безпеки (FAU_STG)

Характеристика сімейства

Сімейство FAU_STG визначає вимоги, при виконанні яких ФБО здатні створювати і супроводжувати журнал аудиту безпеки.

Ранжування компонентів

У FAU_STG.1 "Захищене зберігання журналу аудиту" містить вимоги захисту журналу аудиту від несанкціонованого видалення і / або модифікації.

FAU_STG.2 "Гарантії доступності даних аудиту" визначає гарантії, що ФБО підтримують наявні дані аудиту при виникненні небажаної ситуації.

FAU_STG.3 "Дії в разі можливої втрати даних аудиту" визначає дії, які необхідно зробити, якщо перевищено заданий поріг заповнення журналу аудиту.

FAU_STG.4 "Запобігання втрати даних аудиту" визначає дії при переповненні журналу аудиту.

3.6 Клас FMT. Управління безпекою

Клас FMT призначений для специфікації управління деякими аспектами ФБО: атрибутами безпеки, даними і окремими функціями. Можуть бути встановлені різні ролі управління, а також визначено їх взаємодію, наприклад розподіл обов'язків.

Клас дозволяє вирішувати наступні завдання:

а) Управління даними ФБО, які включають в себе, наприклад, попереджувальні повідомлення.

б) Управління атрибутами безпеки, які включають в себе, наприклад, списки управління доступом і переліки можливостей.

в) Управління функціями з числа ФБО, яке включає в себе, наприклад, вибір функцій, а також правил або умов, що впливають на режим виконання ФБО.

г) Визначення ролей безпеки.

Декомпозиція класу FMT на складові його компоненти приведена на рис. 3.7.

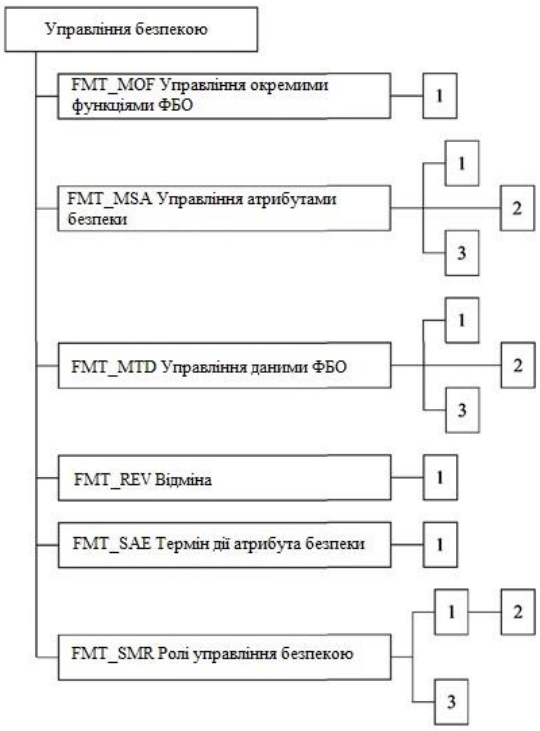


Рисунок 3.7 – Декомпозиція класу FMT «Управління безпекою»

3.6.1 Управління окремими функціями ФБО (FMT_MOF)

Характеристика сімейства

Сімейство FMT_MOF дозволяє уповноваженим користувачам управляти функціями з числа ФБО. До них відносяться, наприклад, функції аудиту та аутентифікації.

Ранжування компонентів

FMT_MOF.1 "Управління режимом виконання функцій безпеки" дозволяє уповноваженим користувачам (ролям) керувати режимом виконання функцій з числа ФБО, що використовують правила або передбачають певні умови, якими можна управляти.

3.6.2 Управління атрибутами безпеки (FMT_MSA)

Характеристика сімейства

Сімейство FMT_MSA допускає уповноважених користувачів до управління атрибутами безпеки. Таке управління може включати в себе можливості перегляду і модифікації атрибутів безпеки.

Ранжування компонентів

FMT_MSA.1 "Управління атрибутами безпеки" дозволяє уповноваженим користувачам (ролям) керувати певними атрибутами безпеки.

FMT_MSA.2 "Безпечні значення атрибутів безпеки" забезпечує, щоб значення, присвоєні атрибутам безпеки, були допустимі з безпеки.

FMT_MSA.3 "Ініціалізація статичних атрибутів" забезпечує, щоб значення атрибутів безпеки за замовчуванням були за своєю суттю або дозволяючими, або обмежувальними.

3.6.3 Управління даними ФБО (FMT_MTD)

Характеристика сімейства

Сімейство FMT_MTD допускає уповноважених користувачів (ролі) до управління даними ФБО. Приклади даних ФБО: інформація аудиту, поточне значення часу, конфігурація системи, інші параметри конфігурації ФБО.

Ранжування компонентів

FMT_MTD.1 "Управління даними ФБО" дозволяє уповноваженим користувачам управляти даними ФБО.

FMT_MTD.2 "Управління обмеженнями даних ФБО" визначає дії, що вживаються при досягненні або перевищенні обмежень даних ФБО.

FMT_MTD.3 "Безпечні дані ФБО" забезпечує, щоб значення, присвоєні даними ФБО, були допустимі з безпеки.

3.6.4 Скасування (FMT_REV)

Характеристика сімейства

Сімейство FMT_REV пов'язано зі скасуванням атрибутів безпеки різних

сутностей в межах ОО.

Ранжування компонентів

FMT_REV.1 "Скасування" передбачає скасування атрибутів безпеки, здійснювану в певний момент часу.

3.6.5 Термін дії атрибута безпеки (FMT_SAE)

Характеристика сімейства

Сімейство FMT_SAE пов'язано з можливістю встановлення терміну дії атрибутів безпеки.

Ранжування компонентів

FMT_SAE.1 "Обмежена за часом авторизація" надає можливість уповноваженому користувачу встановлювати термін дії певних атрибутів безпеки.

3.6.6 Ролі управління безпекою (FMT_SMR)

Характеристика сімейства

Сімейство FMT_SMR призначене для управління призначенням різних ролей користувачам. Можливості цих ролей з управління безпекою описані в інших родинах цього класу.

Ранжування компонентів

FMT_SMR.1 "Ролі безпеки" визначає ролі, пов'язані з безпекою і розпізнаються ФБО.

FMT_SMR.2 "Обмеження на ролі безпеки" визначає, що, на додаток до визначення ролей, є правила, які керують відносинами між ролями.

FMT_SMR.3 "Ухвалення ролей" містить вимогу, щоб прийняття ролі йшло тільки через точний запит до ФБО.

3.7 Клас FTA. Доступ до ОО

Клас FTA визначає функціональні вимоги до управління відкриттям сеансу користувача.

Декомпозиція класу на складові його компоненти приведена на рис. 3.8

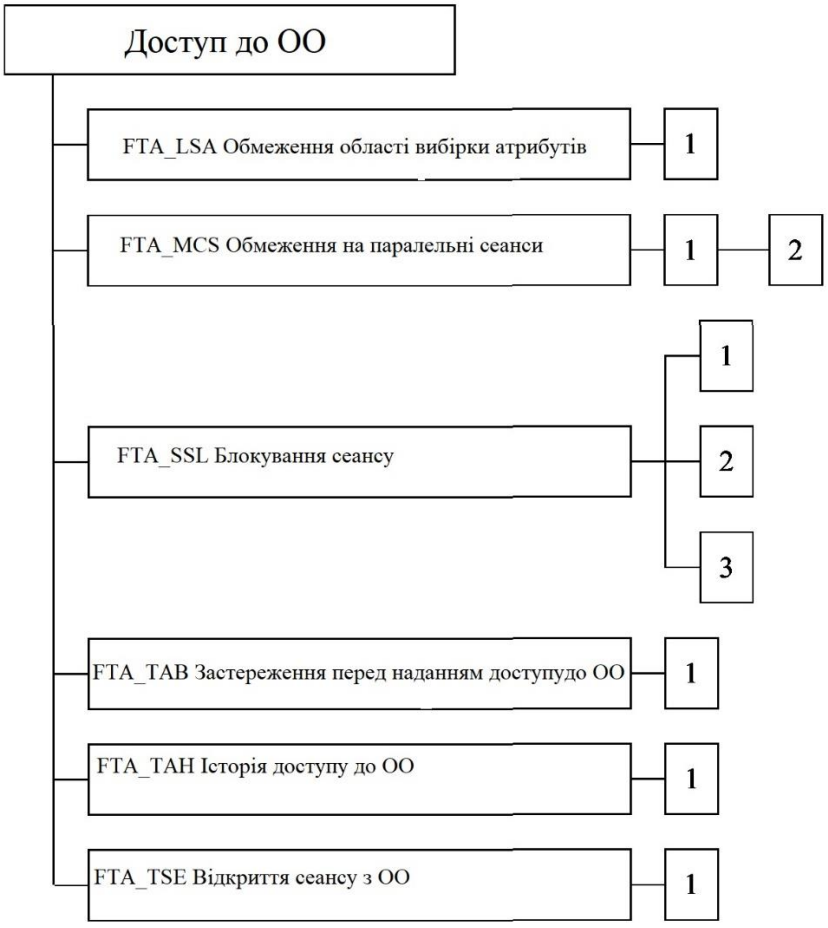


Рисунок 3.8 - Декомпозиція класу FTA «Доступ до ОО»

3.7.1 Обмеження області обраних атрибутів (FTA_LSA)

Характеристика сімейства

Сімейство FTA_LSA визначає вимоги щодо обмеження області атрибутів безпеки сеансу, які може вибирати для нього користувач.

- Ранжування компонентів

FTA_LSA.1 "Обмеження області обираних атрибутів" містить вимогу до ОО щодо обмеження області атрибутів безпеки сеансу під час його відкриття.

3.7.2 Обмеження на паралельні сеанси (FTA_MCS)

Характеристика сімейства

Сімейство FTA_MCS визначає вимоги щодо обмеження числа паралельних сеансів, що надаються одному і тому ж користувачеві.

Ранжування компонентів

FTA_MCS.1 "Базове обмеження на паралельні сеанси" надає обмеження, які застосовуються до всіх користувачів ФБО.

FTA_MCS.2 "Обмеження на паралельні сеанси по атрибутам користувача" розширює FTA_MCS.1 вимогою можливості визначити обмеження на число паралельних сеансів, ґрунтуючись на атрибутах безпеки, пов'язаних з користувачем.

3.7.3 Блокування та завершення сеансу (FTA_SSL)

Характеристика сімейства

Сімейство FTA_SSL визначає вимоги до ФБО з надання можливості як ФБО, так і користувачеві блокувати і розблокувати інтерактивний сеанс.

Ранжування компонентів

FTA_SSL.1 "Блокування сеансу, ініційоване ФБО" включає ініційоване системою блокування інтерактивного сеансу після певного періоду бездіяльності користувача.

FTA_SSL.2 "Блокування, ініційоване користувачем" надає користувачеві можливість блокувати і розблоковувати свої власні інтерактивні сеанси.

FTA_SSL.3 "Завершення, ініційоване ФБО" надає вимоги до ФБО по завершенню сеансу після певного періоду бездіяльності користувача.

3.7.4 Попередження перед наданням доступу до ОО (FTA_TAB)

Характеристика сімейства

Сімейство FTA_TAB визначає вимоги до відображення для користувачів
попереджувального повідомлення з перебудованою конфігурацією щодо характеру використання ОО.

Ранжування компонентів

FTA_TAB.1 "Попередження за замовчуванням перед наданням доступу до ОО" містить вимоги до попереджуючим повідомленнями, які відображаються перед початком діалогу в сеансі.

3.7.5 Історія доступу до ГО (FTA_TAH)

Характеристика сімейства

Сімейство FTA_TAH визначає вимоги до ФБО по відображенню для користувача, при успішному відкритті сеансу, історії успішних і неуспішних спроб отримати доступ від імені цього користувача

Ранжування компонентів

FTA_TAH.1 "Історія доступу до ОО" надає вимоги до ОО по відображенню інформації, пов'язаної з попередніми спробами відкрити сеанс.

3.7.6 Відкриття сеансу з ОО (FTA_TSE)

Характеристика сімейства

Сімейство FTA_TSE визначає вимоги щодо заборони користувачам відкриття сеансу з ОО.

Ранжування компонентів

FTA_TSE.1 "Відкриття сеансу з ОО" надає умови заборони користувачам доступу до ОО, заснованого на атрибутах.

Управління: FTA_TSE.1

Для функцій управління з класу FMT може розглядатися такі дії.

а) Управління уповноваженим адміністратором умовами відкриття сеансу.

Аудит: FTA_TSE.1

Якщо в ПЗ / ЗБ включено сімейство FAU_GEN "Генерація даних аудиту безпеки", то слід передбачити можливість (в залежності від обраного рівня) аудиту наступних дій / подій / параметрів.

а) Мінімальний: заборона відкриття сеансу механізмом відкриття сеансу.

б) Базовий: всі спроби відкриття сеансу користувача.

в) Деталізований: фіксація значень обраних параметрів доступу (таких, як місце доступу або час доступу).

FTA_TSE.1 Відкриття сеансу з ОО

FTA_TSE.1.1 ФБО повинні бути здатні відмовити у відкритті сеансу, ґрунтуючись на [призначення: атрибути].

3.8 Клас FTP. Довірений маршрут / канал

Сімейства класу FTP містять вимоги як до довіреного маршруту зв'язку між користувачами і ФБО, так і до довіреного каналу зв'язку між ФБО й

іншими довіреними продуктами ІТ. Довірені маршрути і канали мають такі загальні властивості:

- маршрут зв'язку створюється з використанням внутрішніх і зовнішніх каналів комунікацій (відповідно до компонентом), які ізолюють ідентифіковане підмножину даних і команд ФБО від решти даних користувачів і ФБО;

- використання маршруту зв'язку може бути ініційовано користувачем або ФБО (відповідно до компоненту);

- маршрут зв'язку здатний забезпечити довіру того, що користувач взаємодіє з необхідними ФБО або ФБО - з необхідним користувачем (відповідно до компоненту).

В даній парадигмі довірений канал - це канал зв'язку, який може бути ініційований будь-якою з зв'язаних сторін і забезпечує властивість неспростовності по відношенню до ідентичності сторін каналу.

Довірений маршрут надає користувачам засоби для виконання функцій шляхом забезпечення прямої взаємодії з ФБО. Довірений маршрут зазвичай бажаний при початковій ідентифікації та / або автентифікації користувача, але може бути також застосований протягом усього сеансу користувача. Обміни по довіреному маршруту можуть бути ініційовані користувачем або ФБО. Гарантується, що відповіді користувача з застосуванням довіреного маршруту будуть захищені від модифікації або розкриття не довіреними додатками.

Декомпозиція класу FTP на складові його компоненти приведена на рис. 3.9

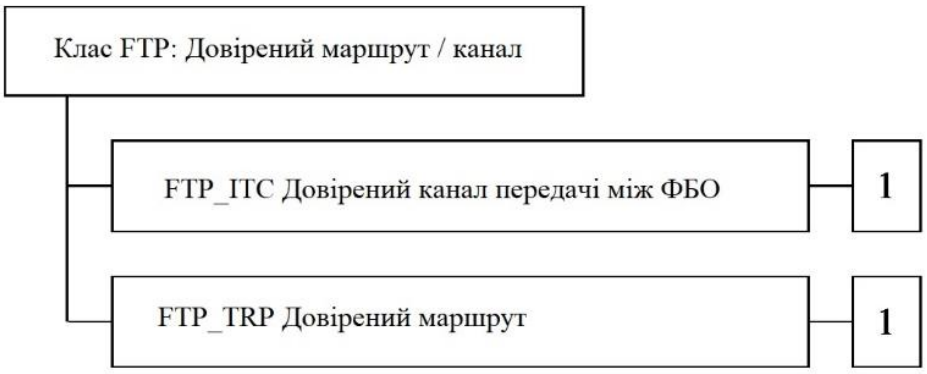


Рисунок 3.9 – Декомпозиція клусу «Довірений маршрут / канал»

3.8.1 Довірений канал передачі між ФБО (FTP_ITC)

Характеристика сімейства

Сімейство FTP_ITC визначає правила створення довіреного каналу між ФБО й іншими довіреними продуктами ІТ для виконання операцій, критичних для безпеки. Це сімейство слід використовувати всякий раз, коли є вимоги безпечної передачі даних користувача або ФБО між ОО та іншими довіреними продуктами ІТ.

Ранжування компонентів

FTP_ITC.1 "Довірений канал передачі між ФБО" містить вимогу, щоб ФБО надали довірений канал зв'язку між ними самими та іншим довіреним продуктом ІТ.

3.8.2 Довірений маршрут (FTP_TRP)

Характеристика сімейства

Сімейство FTP_TRP визначає вимоги установки і підтримки довіреного зв'язку між користувачами і ФБО. Довірений маршрут може знадобитися для будь-якої пов'язаної з безпекою взаємодії. Обмін по довіреному маршруту

може бути ініційований користувачем при взаємодії з ФБО, або ж самі ФБО можуть встановити зв'язок з користувачем по довіреному маршруту.

Ранжування компонентів

FTP_TRP.1 "Довірений маршрут" містить вимогу, щоб довірений маршрут між ФБО і користувачем надавався для сукупності подій, визначених розробником ПЗ / ЗБ. Можливість ініціювати довірений маршрут можуть мати користувач і / або ФБО.

3.9 Клас FRU. Використання ресурсів

Клас FRU містить три сімейства, які підтримують доступність необхідних ресурсів, таких як обчислювальні можливості і / або обсяг пам'яті. Сімейство FRU_FLT "Відмовостійкість" надає захист від недоступності ресурсів, викликаної збоєм ОО. Сімейство FRU_PRS "Пріоритет обслуговування" забезпечує, щоб ресурси виділялися найбільш важливим або критичним за часом завданням і не могли бути монополізовані завданнями з більш низьким пріоритетом. Сімейство FRU_RSA "Розподіл ресурсів" встановлює обмеження використання доступних ресурсів, запобігаючи монополізацію ресурсів користувачами.

Декомпозиція класу FRU на складові його компоненти приведена на рис. 3.10

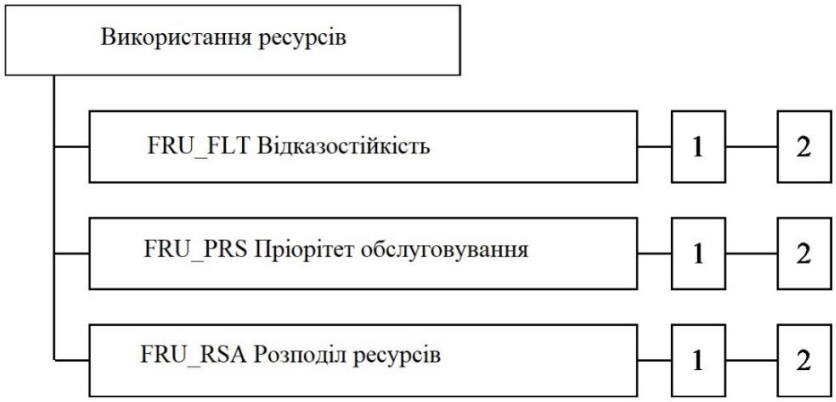


Рисунок 3.10 - Декомпозиція класу FRU «Використання ресурсів»

3.9.1 Відмовостійкість (FRU_FLT)

Характеристика сімейства

Вимоги сімейства FRU_FLT забезпечують, щоб ОО продовжив підтримувати правильне функціонування навіть у разі збоїв.

Ранжування компонентів

FRU_FLT.1 "Знижена відмовостійкість" містить вимогу, щоб ОО продовжив правильне виконання зазначених можливостей в разі ідентифікованих збоїв.

FRU_FLT.2 "Обмежена відмовостійкість" містить вимогу, щоб ОО продовжив правильне виконання всіх своїх можливостей в разі ідентифікованих збоїв.

3.9.2 Пріоритет обслуговування (FRU_PRS)

Характеристика сімейства

Вимоги сімейства FRU_PRS дозволяють ФБО управляти використанням ресурсів користувачами та суб'єктами в межах своєї області дії так, щоб високо пріоритетні операції в межах ОДФ завжди будуть виконуватися без перешкод або затримок з боку операцій з більш низьким пріоритетом.

Ранжування компонентів

FRU_PRS.1 "Обмежений пріоритет обслуговування" надає пріоритети для використання суб'єктами підмножини ресурсів в межах ОДФ.

FRU_PRS.2 "Повний пріоритет обслуговування" надає пріоритети для використання суб'єктами всіх ресурсів в межах ОДФ.

3.9.3 Розподіл ресурсів (FRU_RSA)

Характеристика сімейства

Вимоги сімейства FRU_RSA дозволяють ФБО управляти використанням ресурсів користувачами та суб'єктами таким чином, щоб не відбувалося відмов в обслуговуванні через несанкціоновану монополізацію ресурсів.

Ранжування компонентів

FRU_RSA.1 "Максимальні квоти" містить вимоги до механізмів квотування, які забезпечують, щоб користувачі і суб'єкти не монополізували керований ресурс.

FRU_RSA.2 "Мінімальні та максимальні квоти" містить вимоги до механізмів квотування, які забезпечують, щоб користувачі і суб'єкти завжди мали хоча б мінімум специфікованого ресурсу, але при цьому не могли б монополізувати цей ресурс.

3.10 Клас FPR. Конфіденційність

Клас FPR містить вимоги конфеденційності. Ці вимоги надають користувачеві захист від розкриття його ідентифікатора і зловживання цим іншими користувачами.

Декомпозиція класу FPR на складові його компоненти приведена на рис. 3.11

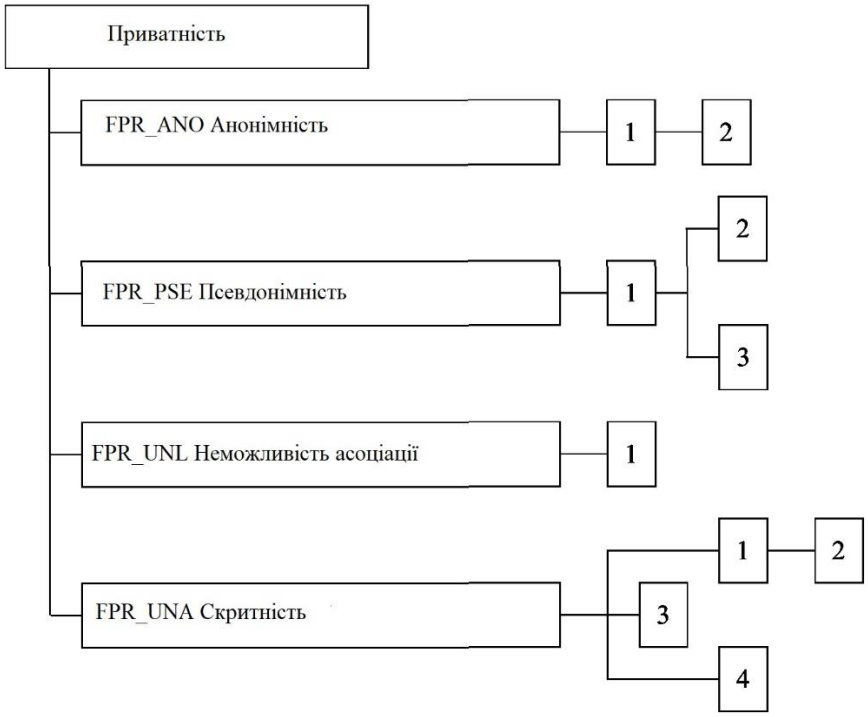


Рисунок 3.11 – Декомпозиція класу FPR «Приватність»

3.10.1 Анонімність (FPR_ANO)

Характеристика сімейства

Сімейство FPR_ANO забезпечує, щоб користувач міг використовувати ресурс або послугу ОО без розкриття свого ідентифікатора. Вимоги сімейства надають захист ідентифікатора користувача. Сімейство не призначене для захисту ідентифікаторів суб'єктів.

Ранжування компонентів

FPR_ANO.1 "Анонімність" містить вимогу, щоб інші користувачі або суб'єкти не могли визначити ідентифікатор користувача, пов'язаного з суб'єктом або операцією.

FPR_ANO.2 "Анонімність без запиту інформації" розширює вимоги FPR_ANO.1, «анонімність», забезпечуючи, щоб ФБО не запитували ідентифікатор користувача.

3.10.2 Псевдонімність (FPR_PSE)

Характеристика сімейства

Сімейство FPR_PSE забезпечує, щоб користувач міг використовувати ресурс або послугу без розкриття свого ідентифікатора, залишаючись в той же час відповідальним за це використання.

Ранжування компонентів

FPR_PSE.1 "псевдонімного" містить вимогу, щоб деяка сукупність користувачів і / або суб'єктів була не здатна визначити ідентифікатор користувача, пов'язаного з суб'єктом або операцією, але в той же час цей користувач залишався відповідальним за свої дії.

FPR_PSE.2 "Оборотна псевдонімного" містить вимогу, щоб ФБО надали можливість визначити початковий ідентифікатор користувача, ґрунтуючись на представленому псевдонімі.

FPR_PSE.3 "Альтернативна псевдонімного" містить вимогу, щоб при створенні псевдоніма для ідентифікатора користувача ФБО слідували певним правилам.

3.10.3 Неможливість асоціації (FPR_UNL)

Характеристика сімейства

Сімейство FPR_UNL забезпечує, щоб користувач міг неодноразово використовувати ресурси або послуги, не даючи в той же час нікому можливості зв'язати разом їх використання.

Ранжування компонентів

FPR_UNL.1 "Неможливість асоціації" містить вимогу, щоб користувачі або суб'єкти були не здатні визначити, чи були певні операції в системі ініційовані одним і тим же користувачем.

3.10.4 Скритність (FPR_UNO)

Характеристика сімейства

Сімейство FPR_UNO забезпечує, щоб користувач міг використовувати ресурс або послугу без надання будь-кому, особливо третій стороні, інформації про використання ресурсу або послуги.

Ранжування компонентів

FPR_UNO.1 "Скритність" містить вимогу, щоб користувачі і / або суб'єкти не могли визначити, чи виконується операція.

FPR_UNO.2 "Розподіл інформації, що впливає на скритність" містить вимогу, щоб ФБО надали спеціальні механізми для запобігання концентрації інформації, пов'язаної з приватних даних, в межах ОО. Така концентрація могла б вплинути на забезпечення скритності при порушеннях безпеки.

FPR_UNO.3 "Скритність без запиту інформації" містить вимогу, щоб ФБО не намагалися отримати інформацію, пов'язану з приватних даних, що може використовуватися для порушення скритності.

FPR_UNO.4 "Відкритість для уповноваженого користувача" містить вимогу, щоб ФБО надали одному або декільком уповноваженим користувачам можливість спостерігати за використанням ресурсів і / або послуг.

3.11 Клас FPT. Захист ФБО

Клас FPT містить сімейства функціональних вимог, які пов'язані з цілісністю і управлінням механізмами, реалізованими в ФБО, що при цьому не залежать від особливостей ПБО, а також з цілісністю даних ФБО, що не залежити від специфічного змісту даних ПБО. У певному сенсі, компоненти сімейств цього класу дублюють компоненти з класу FDP і можуть навіть використовувати одні і ті ж механізми. Однак клас FDP спеціалізований на захист даних користувача, в той час як клас FPT націлений на захист даних

ФБО. Фактично, компоненти з класу FPT необхідні для забезпечення вимог неможливості порушення і обходу політик ФБ даного ОО.

В рамках цього класу виділяються три істотні складові частини ФБО.

а) Абстрактна машина ФБО, тобто віртуальна або фізична машина, на якій виконується оцінювана реалізація ФБО.

б) Реалізація ФБО, яка виконується на абстрактної машині і реалізує механізми, які здійснюють ПБО.

в) Дані ФБО, які є адміністративними базами даних, які керують здійсненням ПБО.

Декомпозиція класу FPT на складові його компоненти приведена на рисунку 3.12

Характеристика сімейства

Сімейство FPT_AMT визначає вимоги до виконання тестування ФБО, який демонструє припущення безпеки щодо базової абстрактної машини, на яку покладається ФБО. "Абстрактна" машина може бути як платформою апаратних / програмно-апаратних засобів, так і деяким відомим і пройденим оцінку поєднанням апаратних / програмних засобів, що діють як віртуальна машина.

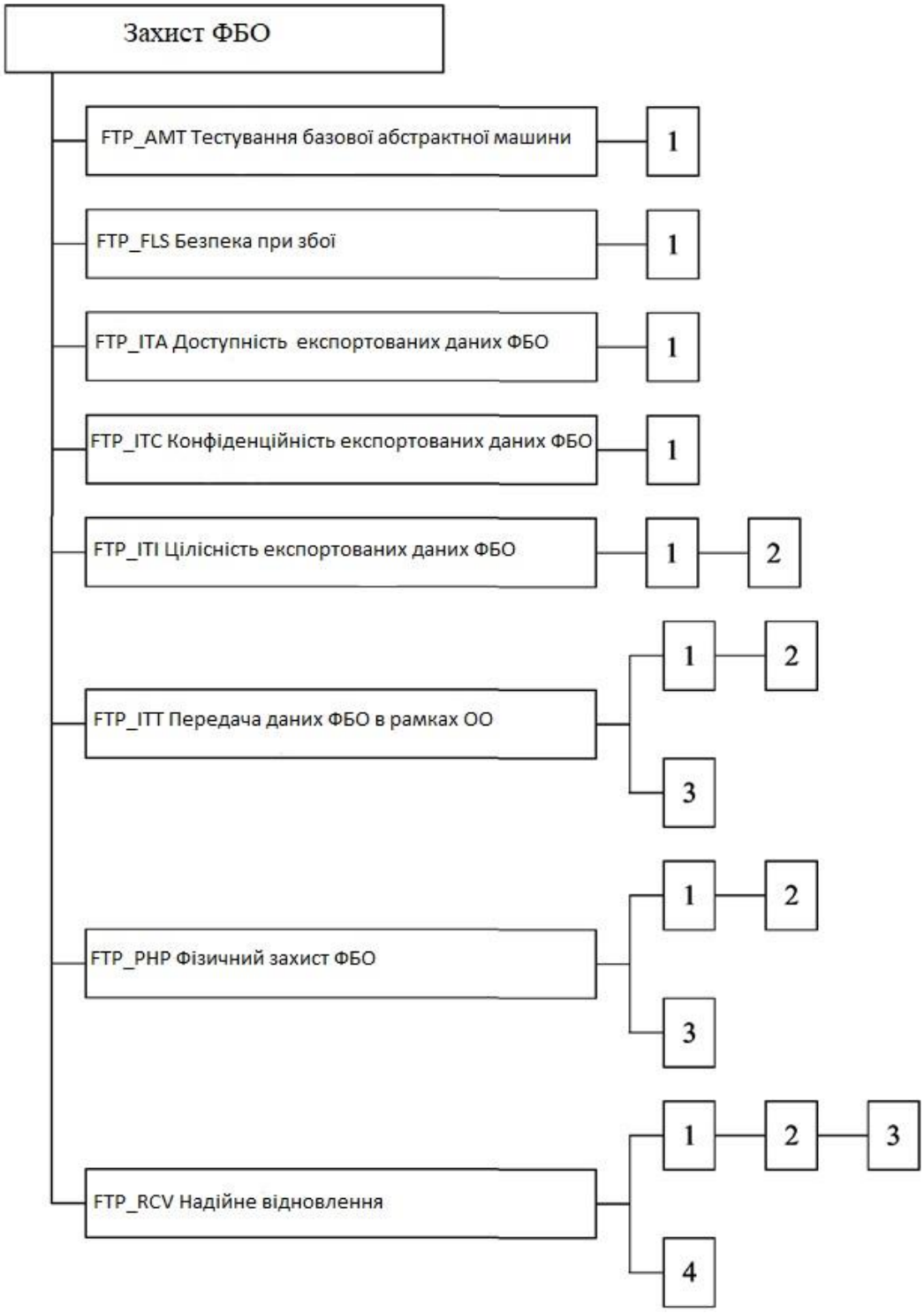


Рисунок 3.12 – Декомпозиція класу « Захист ФБО»

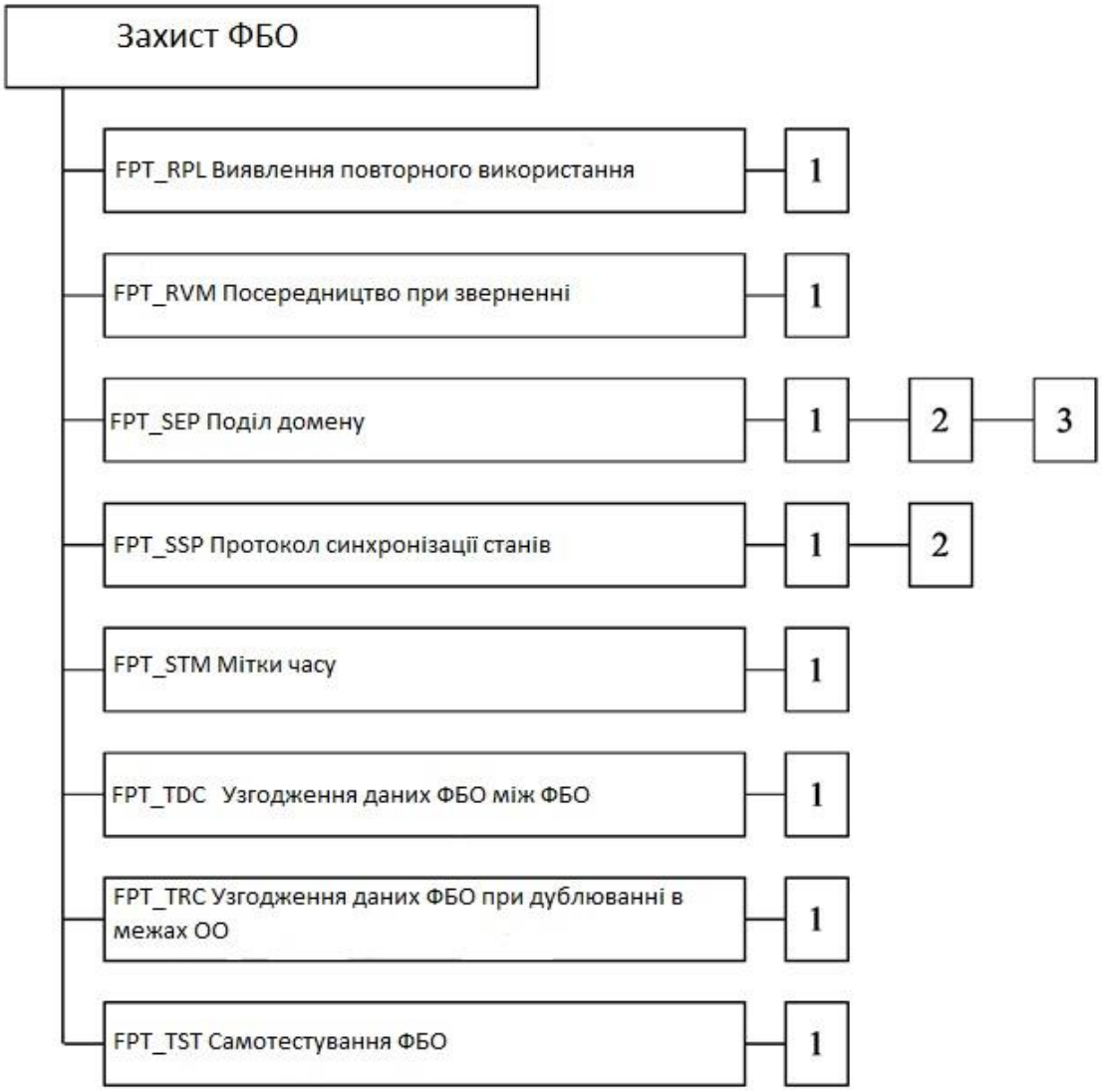


Рисунок 3.12 (продовження)

3.11.1 Тестування базової абстрактної машини (FPT_AMT)

Ранжування компонентів

FPT_AMT.1 Тестування абстрактної машини

FPT_AMT.1.1 ФБО повинні виконувати пакет тестових програм під час запуску, за запитом Адміністратора кошти побудови ВЛВС, для демонстрації правильності виконання припущень безпеки, які забезпечуються абстрактною машиною, яка покладена в основу ФБО.

3.11.2 Безпека при збої (FPT_FLS)

FPT_FLS.1 Збій зі збереженням безпечного стану

FPT_FLS.1.1 ФБО повинні зберегти безпечний стан при наступних типах збоїв: збій в системі електроживлення ОО, виявлення порушення безпеки.

3.11.3 Надійне відновлення (FPT_RCV)

FPT_RCV.2 Автоматичне відновлення

FPT_RCV.2.1 Коли автоматичне відновлення після збою або переривання обслуговування неможливо, ФБО повинні перейти в режим аварійної підтримки, який надає можливість повернення ОО до безпечного стану.

FPT_RCV.2.2 Для збоїв в системі електроживлення ОО ФБО повинні забезпечити повернення ОО до безпечного стану з використанням автоматичних процедур.

FPT_RPL.1.2 ФБО повинні відмовити в доступі, зробити генерацію записи журналу аудиту, передачу запису журналу аудиту САС, здійснити сигналізацію Адміністратору кошти побудови ВЛВС про можливе порушення безпеки, при виявленні повторного використання.

3.11.4 Посередництво при зверненнях (FPT_RVM)

FPT_RVM.1 Неможливість обходу ПБ ОО

FPT_RVM.1.1 ФБО повинні забезпечити, щоб функції, які здійснюють ПБО викликалися і успішно виконувалися раніше, ніж дозволяється виконання будь-якої іншої функції в межах області дії ФБО.

3.11.5 Поділ домену (FPT_SEP)

FPT_SEP.1 Відділення області ФБО

FPT_SEP.1.1 ФБО повинні підтримувати домен безпеки для власного виконання, який захищає їх від втручання і спотворення не довірених суб'єктів.

FPT_SEP.1.2 ФБО повинні реалізувати поділ між доменами безпеки суб'єктів в області дії ФБО.

3.11.6 Мітки часу (FPT_STM)

FPT_STM.1 Надійні мітки часу

FPT_STM.1.1 ФБО повинні бути здатні надати надійні мітки часу для власного використання.

Примітка 1: Поняття "надійні" в даній вимозі означає чітке збереження порядку проходження подій, що реєструються ОО, з урахуванням дати і часу.

3.11.7 Узгодженість даних ФБО між ФБО (FPT_TDC)

FPT_TDC.1 Взаємна базова узгодженість даних ФБО

FPT_TDC.1.1 ФБО повинні забезпечити здатність злагоджено інтерпретувати дані журналу аудиту, значення ідентифікаторів ВЛВС, спільно використовувані ФБО і іншим довіреним продуктом ІТ.

FPT_TDC.1.2 ФБО повинні використовувати певні протоколи взаємодії, (специфіковані в ЗБ) при інтерпретації даних ФБО, отриманих від іншого довіреної продукту ІТ.

3.11.8 Самотестування ФБО (FPT_TST)

FPT_TST.1 Тестування ФБО

FPT_TST.1.1 ФБО повинні виконувати пакет програм самотестування при запуску, періодично в процесі нормального функціонування, за запитом Адміністратора кошти побудови ВЛВС, для демонстрації правильного виконання ФБО.

FPT_TST.1.2 ФБО повинні надати Адміністратору кошти побудови ВЛВС можливість верифікувати цілісність даних ФБО.

FPT_TST.1.3 ФБО повинні надати Адміністратору кошти побудови ВЛВС можливість верифікувати цілісність зберігається виконуваного коду ФБО.

3.12 Висновки до розділу 3

Стандарт ISO/IEC 15408 та відповідні функціональні вимоги безпеки, описані вище, не призначені для остаточного вирішення всіх завдань безпеки ІТ. Швидше пропонує сукупність добре продуманих функціональних вимог безпеки, які можуть застосовуватися при створенні систем ІТ.

У подальшому потреби користувачів можуть змінюватися, тому функціональні вимоги, представлені в цьому стандарті, потребують подальшого удосконалення. Можливо деякі розробники ПЗ/ЗБ можуть мати потреби в безпеці, яку компоненти функціональних вимог представлені в цьому стандарті не зможуть охопити. Тоді розробник ПЗ/ЗБ може спробувати використати нестандартні функціональні вимоги (так звану "розширюваність") відповідно до ISO / IEC 15408-1, додатки A і B.

4 СЕРТИФІКАЦІЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ВІДПОВІДНІСТЬ ISO 15408

4.1 Сертифікація

Для протидії загрозам безпеки компаніями застосовується комплексний підхід з організаційних і технічних заходів. Вибір засобів захисту визначається в результаті аналізу загроз і ступеня захищеності об'єкта.

У споживачів в сфері IT є різні варіанти визначення рівня безпеки їх продуктів і систем:

- довіритися виробнику продукту / послуг,

- протестувати систему самостійно,

- покластися на оцінку з боку незалежного органу (оцінка відповідності, - сертифікація).

Розглянемо третій варіант і дамо загальне уявлення про механізми і принципи сертифікації безпеки в сфері IT.

4.2 Загальні аспекти сертифікація систем інформаційної безпеки

Сертифікація безпеки - це форма підтвердження відповідності об'єктів вимогам технічних регламентів, положенням стандартів, зводів правил або умов договорів.

Мета сертифікації полягає в забезпеченні впевненості споживача продукту IT в тому, що він забезпечує виконання всіх заявлених функціональних можливостей безпеки і це підтверджується незалежними випробуваннями спеціального органу. Незалежним органом виступає, як правило, акредитований орган з оцінки відповідності. В Україні таким органом з акредитації є Національне агентство з акредитації України.

Сертифікація інформаційної безпеки може стосуватись як процедурних питань (сертифікація систем управління інформаційною безпекою на

відповідність стандарту ISO 27001:2013) так і на технічному рівні, - продуктів ІТ та систем ІБ (як правило, на відповідність ISO 15408).

Найзначнішим в цьому плані документом є міжнародний стандарт ISO 15408 «Критерії оцінки безпеки інформаційних технологій» або коротко - Загальні Критерії (ЗК). Треба підкреслити, що положення ЗК носять досить загальний характер. По суті, Загальні критерії не містять вимог до конкретних систем захисту інформації, а являють собою набір визначень і правил, в рамках яких можна описувати різні системи захисту.

На основі ЗК споживач може вибрати продукт, який відповідає його потребам, а також сформулювати свої вимоги до безпеки виробникам. Документ корисний і як керівництво при розробці, причому не тільки спеціалізованих засобів захисту, а й будь-якого ПЗ або апаратних засобів з функціями безпеки. Експерти по сертифікації розглядають стандарти як інструмент, що дозволяє їм оцінити рівень безпеки, що забезпечується продуктами ІТ, і надати споживачам можливість зробити обґрунтований вибір.

Загальні критерії складаються з чотирьох частин

- Введення і загальна модель

У ній визначаються загальні поняття, концепції безпеки, принципи оцінки безпеки ІТ, наводиться загальна модель оцінки. Ця частина також складає основні структури для запису вимог безпеки: пакет, профіль захисту (ПЗ) і завдання з безпеки (ЗБ).

- Функціональні вимоги безпеки

Вона містить систематизований каталог функціональних компонентів. Функціональні компоненти використовуються в якості стандартних шаблонів, на основі яких слід встановлювати функціональні вимоги до оцінюваного продукту.

- Вимоги довіри до безпеки

Ця частина містить каталог вимог довіри, систематизованих за сімействами і класам. Крім того, в ній визначені критерії оцінки профілів

захисту і завдань з безпеки і представлені сім зумовлених пакетів довіри, т.зв. «Оціночних рівнів довіри» (ОРД). ОРД 1 забезпечує найнижчий рівень довіри, ОРД7 - найвищий. Із зростанням порядкового номера пред'являються вимоги посилюються.

Таким чином, на основі ОК, випробувальна лабораторія (орган сертифікації) перевіряє функціональні можливості безпеки і оцінює, чи відповідають вони описаним в специфікації.

Процес випробувань функціональних можливостей безпеки в лабораторії схожий на процес звичайного тестування, за винятком того, якщо функцій безпеки продукту і засвідчується, що продукт перебуває в заданому середовищі функціонування.

Важливою умовою для початку випробувань є створення випробувального стенду, в якому сам оцінюваний продукт і середовище його функціонування повинні строго відповідати описуваної в завданні з безпеки конфігурації. Також необхідно розробити тестову документацію на підставі ЗБ і функціональної специфікації. З'ясувавши з документів очікуваний режим виконання функцій безпеки, необхідно визначити найбільш підходящий спосіб їх тестування.

Ретельно перевіряють

- Підхід, який буде використовуватися, наприклад, зовнішній інтерфейс, внутрішній інтерфейс, чи будуть задіяні будь-які засоби автономного тестування або альтернативний підхід тестування (наприклад, у виняткових обставинах - ревю коду, якщо експерт це може);

- Інтерфейс який буде використовуватися для тестування і спостереження за реакціями інтерфейсу;

- Початкові умови, необхідні для виконання тесту (тобто будь-які конкретні об'єкти або суб'єкти, які будуть необхідні, і атрибути безпеки, які їм необхідно буде мати);

- Спеціальне обладнання для тестування, або для ініціювання функції безпеки (наприклад, генератори пакетів), або для спостереження за функцією безпеки (наприклад, мережеві аналізатори).

Лабораторія (орган) може вважати за доцільне протестувати кожен інтерфейс функцій безпеки, використовуючи ряд тестів, де кожен тест буде використовуватися для перевірки дуже специфічного аспекту очікуваного режиму функціонування інтерфейсу.

Експерти лабораторії, також, для встановлення відповідності вимогам довіри виконують пошук потенційних вразливостей в продукті і середовищі функціонування, використовуючи всі доступні джерела. Грунтуючись на проведеному пошуку потенційних вразливостей, розробляються і виконуються тести на проникнення.

Результати тестування вносяться в спеціальний звіт з включенням інформації про витрачені зусилля на тести по проникненню, про всі придатних для використання вразливості, рівень компетентності зловмисника, рівні знання продукту, обладнанні, необхідних для використання ідентифікованих вразливостей.

Лабораторія досліджує всі результати проведених випробувань, робить відповідний висновок і виносить свою оцінку. Результати такої оцінки є основою для офіційної сертифікації продукту.

Можна зробити висновки що до сертифікації:

Сертифікація по ЗК і тестування безпеки, як процеси, безумовно, пов'язані. Однак тестування безпеки може проводитися або не проводитися (це залежить від бажання замовника). Доказів, гарантій безпеки покупцеві таке тестування безпеки не дає.

Сертифікація, в свою чергу, часто є обов'язковою процедурою (особливо для державних установ) і надає повну гарантію виконання функцій безпеки.

4.3 Готовність сертифікації систем інформаційної безпеки на відповідність ISO 15408 в Україні

Сертифікація на відповідність ЗК (Common Criteria – CC) по ISO 15408 як правило визначається для IT – закупівель, ліцензування, введення обьектів в експлуатацію тощо.

Інші стандарти, що містить, наприклад, інтероперабельність, управління системою ІБ, навчання користувачів сертифікуються на інші стандарти. Приклади включають ISO/IEC 17799 (або більш правильно BS 7799-1, який в даний час є ISO/IEC 27002) або німецький IT-Grundschutzhandbuch, тощо.

ЗК (CC) виникли з трьох стандартів:

- ITSEC - Європейський стандарт, розроблений такими країнами як Франція, Німеччина, Нідерланди і Великобританія на початку 1990 - х років. Це також було об'єднанням ранніх робіт, таких як два британських підходи (CESG Великобританія Схеми оцінки, спрямовані на захист / ринку розвідки і DTI Зеленій книзі, спрямованої на комерційне використання), і було прийнято в деяких інших країнах, наприклад, в Австралії.

- CTCPEC - Канадський стандарт пішов з стандарту US DoD, але зміг уникнути ряду проблем, і була використана спільно, оцінювачами з США і Канади. Стандарт CTCPEC вперше був опублікований в травні 1993 року.

- TCSEC - The США Міністерство оборони DoD 5200.28 Std, називається Orange Book і є частиною серії «Радуга». Помаранчева книга виникла із робіт по комп'ютерній безпеці, включаючи звіт Андерсона, зроблену в Агентстві національної безпеки і Національне бюро стандартів (НБС в кінцевому підсумку став NIST) в кінці 1970 - х і початку 1980 - х років. Центральна теза Помаранчевої книги випливає з роботи, виконаної Дейв Белл і Льон ЛаПадула для набору механізмів захисту.

CC був створений шляхом об'єднання раніше існуючих стандартів, в основному так, що компанії з продажу комп'ютерної продукції для

державного ринку (в основному для оборони або розвідок) мали *оцінювати* тільки одним набором стандартів. CC був розроблений урядами Канади, Франції, Німеччини, Нідерландів, Великобританії та США.

Всі випробувальні лабораторії для акредитації повинні відповідати ISO 17025, а органи з сертифікації, як правило, затверджуються (акредитуються) на основі ISO/IEC Guide 65 або BS EN 45011 (зараз це ISO 17065). Відповідність вимогам ISO 17025 або ISO 17065, як правило, відбувається на рівні національного офіційного затвердження органами акредитації:

- У Канаді Рада зі стандартів Канади (SCC) в рамках Програми з акредитації лабораторій (PALCAN) акредитує Загальні критерії оцінки споруди (CCEF)

- У Франції Comité français d'АКРЕДИТАЦІЯ (COFRAC) акредитує Загальні засоби оцінки Критеріїв. Оцінки здійснюються відповідно до норм і стандартів, встановлених Національним агентством де ла sécurité де Systemes d'інформації

- У Великобританії: служба акредитації Великобританії, Акредитація (UKAS) акредитує Комерційну оцінку Послуги (ключі)

- У США, Національний інститут стандартів і технології (NIST) Національна акредитаційна Програма добровільного Laboratory (NVLAP) акредитує Common Criteria Testing Laboratories (КЦТЛ)

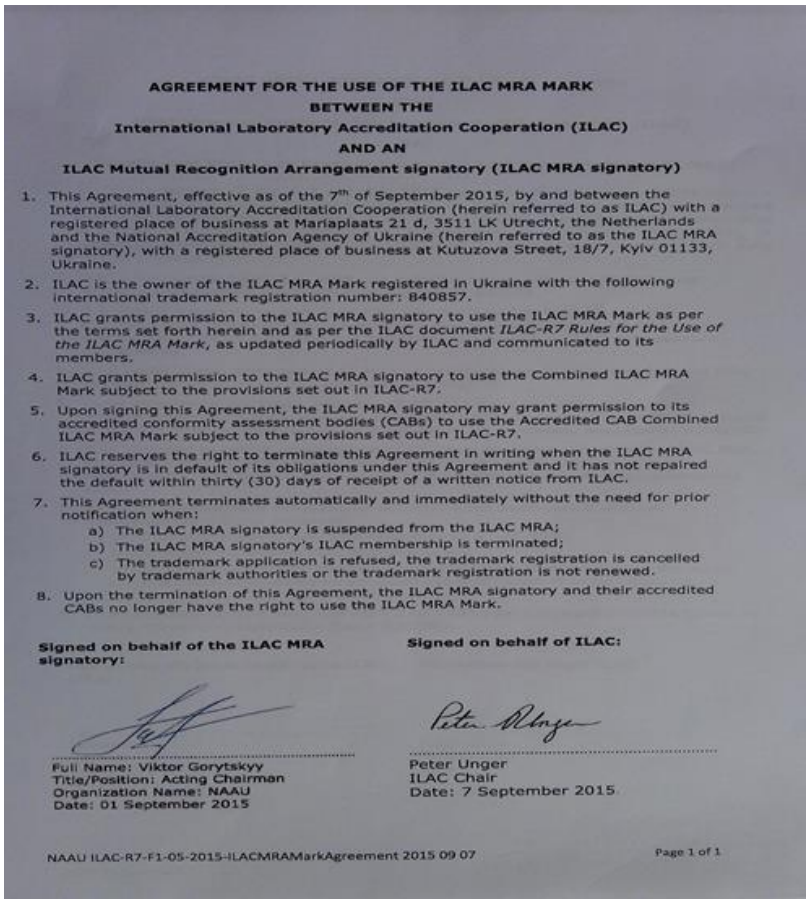
- У Німеччині Bundesamt für Sicherheit в дер Informationstechnik (BSI)

- В Іспанії, Національний Кріптолоджік центр (CCN) акредитує Common Criteria випробувальних лабораторій, що працює в іспанській схемою.

- У Нідерландах схема Нідерландів по сертифікації в сфері IT - безпеки (NSCIB) акредитує IT Security Evaluation Послуги (ITSEF).

В Україні випробувальні лабораторії (на ISO 17025) та органи сертифікації (на ISO 17065) акредитує Національне агентство з акредитації України (НААУ), яке має визнання у вигляді Угод про визнання результатів акредитації для лабораторій по ISO 17025 та органів сертифікації по ISO

17065 для європейського (EA) та глобального рівнів ILAC та IAF (Рис. 4.1 – 4.4).



AGREEMENT FOR THE USE OF THE ILAC MRA MARK
BETWEEN THE
International Laboratory Accreditation Cooperation (ILAC)
AND AN
ILAC Mutual Recognition Arrangement signatory (ILAC MRA signatory)

1. This Agreement, effective as of the 7th of September 2015, by and between the International Laboratory Accreditation Cooperation (herein referred to as ILAC) with a registered place of business at Mariaplaats 21 d, 3511 LK Utrecht, the Netherlands and the National Accreditation Agency of Ukraine (herein referred to as the ILAC MRA signatory), with a registered place of business at Kutuzova Street, 18/7, Kyiv 01133, Ukraine.
2. ILAC is the owner of the ILAC MRA Mark registered in Ukraine with the following international trademark registration number: 840857.
3. ILAC grants permission to the ILAC MRA signatory to use the ILAC MRA Mark as per the terms set forth herein and as per the ILAC document *ILAC-R7 Rules for the Use of the ILAC MRA Mark*, as updated periodically by ILAC and communicated to its members.
4. ILAC grants permission to the ILAC MRA signatory to use the Combined ILAC MRA Mark subject to the provisions set out in ILAC-R7.
5. Upon signing this Agreement, the ILAC MRA signatory may grant permission to its accredited conformity assessment bodies (CABs) to use the Accredited CAB Combined ILAC MRA Mark subject to the provisions set out in ILAC-R7.
6. ILAC reserves the right to terminate this Agreement in writing when the ILAC MRA signatory is in default of its obligations under this Agreement and it has not repaired the default within thirty (30) days of receipt of a written notice from ILAC.
7. This Agreement terminates automatically and immediately without the need for prior notification when:
   a) The ILAC MRA signatory is suspended from the ILAC MRA;
   b) The ILAC MRA signatory's ILAC membership is terminated;
   c) The trademark application is refused, the trademark registration is cancelled by trademark authorities or the trademark registration is not renewed.
8. Upon the termination of this Agreement, the ILAC MRA signatory and their accredited CABs no longer have the right to use the ILAC MRA Mark.

Signed on behalf of the ILAC MRA signatory:

Full Name: Viktor Gorytskyy
Title/Position: Acting Chairman
Organization Name: NAAU
Date: 01 September 2015

Signed on behalf of ILAC:

Peter Unger
ILAC Chair
Date: 7 September 2015

NAAU ILAC-R7-F1-05-2015-ILACMRAMarkAgreement 2015 09 07 Page 1 of 1

Рисунок 4.1 - Співробітництво з ILAC – Угода про взаємне визнання

International Accreditation Forum, Inc. (IAF)

Be it known that the

NATIONAL ACCREDITATION AGENCY OF UKRAINE (NAAU), UKRAINE

has been accepted as a Member of the

International Accreditation Forum, Inc.
Multilateral Recognition Arrangement

for the following:

Main Scope: Product Certification - ISO/IEC 17065 (16 August 2017)
Main Scope: Certification of Persons - ISO/IEC 17024 (16 August 2017)
Main Scope: Management System Certification - ISO/IEC 17021-1
Sub-Scopes: Level 5: ISO 9001 (16 August 2017)
Level 5: ISO 14001 (16 August 2017)

The Member on behalf of which this sheet is signed commits itself to comply with the requirements and obligations of Members of the IAF MLA.

Viktor Gorytskyy
Chairman,
National Accreditation Agency of Ukraine
DATE: 16 August 2017

Xiao Jianhua
Chairman,
International Accreditation Forum, Inc.
DATE: 16 August 2017

Рисунок 4.2 - Співробітництво з IAF – Угода про взаємне визнання

NAAU – 068

Signed on behalf of National Accreditation Agency of Ukraine (NAAU)

(*Signature*)

Dr. Viktor Gorytskyy
Chairman

Date: 6 September 2017

(*Signature*)

Xiao Jianhua
Chairman of IAF

Date: 6 September 2017

IAF MLA Mark License

Licensed to use the IAF MLA Mark for IAF recognized main scopes and sub-scopes as individually listed and updated on the IAF Members and Signatories page of the IAF website, www.iaf.nu.

ML 2:2016, Issue 3

Рисунок 4.3 - Співробітництво з IAF – Договір про використання знаку IAF MLA

EUROPEAN ACCREDITATION

Extension of
Bilateral Agreement

NAAU (BLA) *National Accreditation Agency of Ukraine*
UKRAINE

SCOPE OF RECOGNITION		EA MLA Council decision date
ACCREDITATION ACTIVITY		
EA MLA Level 2: Activity	EA MLA Level 3: Standard	
Testing	EN ISO/IEC 17025	19 April 2012
Calibration	EN ISO/IEC 17025	19 April 2012
Inspection	EN ISO/IEC 17020	3 October 2014
Product certification	EN ISO/IEC 17065	2 October 2015
Certification of persons	EN ISO/IEC 17024	2 October 2015
Management system certification	EN ISO/IEC 17021	19 April 2012

Name Viktor Gorytskyy
Position *Acting Chairman of NAAU*

Authorised signature on behalf of above Accreditation Body

Nicole Meurée-Vanlaethem
Chair of EA MLA Council

Authorised signature on behalf of EA MLA Signatories

Рисунок 4.4 - Співробітництво з Європейською кооперацією з акредитації (ЕА)

4.4 Висновки

Таким чином Україна на сьогодні володіє інструментарієм, який може бути використаний для оцінки відповідності (сертифікації) систем ІБ на відповідність ISO 15408 таким чином, що результати сертифікації можуть бути прийняті на міжнародному глобальному рівні серед країн-підписантів Угоди про взаємне визнання для організацій IAF (на ISO 17065) та ILAC (на ISO 17025).

ВИСНОВКИ

Отже можна зробити висновок що "Загальні критерії" насправді є метастандартом, визначаючим інструменти оцінки безпеки і порядок їх використання .Забезпечення безпечного функціонування IT-систем вимагає вдосконалення методів оцінки реального рівня безпеки та відповідності вимогам нормативної бази та специфікації. Як показав аналіз, найбільш досконалий з існуючих в даний час стандартів є міжнародний стандарт ISO / IEC 15408.

Загальні критерії можна вважати набором бібліотек, які допомагають писати типові профілі захисту, змістовні "програми" - завдання з безпеки, і т.д. Бібліотека спрощує розробку програм та підвищує їх якість

У подальшій перспективі є необхідність розвивати і вдосконалювати існуючі моделі і методи оцінки, розробляти більш універсальні і гнучкі методики для використання в різних системах, а також підвищувати рівень формалізації процесу оцінки і обґрунтування безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального [...] Мін'юст України, Адміністрація Держспецзв’язку; Наказ, Перелік від 25.12.2014 № 2170/5/703.

2. International Organization for Standardization [Електронний ресурс]// – Режим доступу: http://www.iso.org/iso/home.html.

3. ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

6. ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components.

7. Технології комп’ютерної безпеки: монографія / А. В. Погребняк– Рівне : МЕГУ, 2011. – 117 с.

8. НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.